UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Filip Božić

Človeški dejavnik pri zagotavljanju informacijske varnosti

MAGISTRSKO DELO

Ljubljana, 2016

ZAHVALA

Iskreno se zahvaljujem mentorju prof. dr. Denisu Trčku za strokovno usmerjanje in znanstvene napotke. Za končno jezikovno dovršenost hvala lektorici univ. dipl. slov. Špeli Mlinar.

In ne nazadnje – brez podpore, potrpljenja in pomoči bližnjih bi bila pot do magistrskega naziva nemogoča, zato tudi vam ljubeča hvala!

Filip

UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Filip Božić

Človeški dejavnik pri zagotavljanju informacijske varnosti

Magistrsko delo

Mentor: prof. dr. Denis Trček

Ljubljana, 2016

Kazalo

Povzetek

Velik pomen, ki ga družba namenja varovanju informacij, narekuje predvsem hiter razvoj tehnologije. Tehnološke rešitve v veliki meri omogočajo varovanje informacij, to je zaupnosti, celovitosti in razpoložljivosti. Ravno zaradi napredka tehnologije pa je čedalje bolj izpostavljen (ali celo zapostavljen) človeški dejavnik, ne nazadnje mora tudi s tehnologijo ravnati — človek. Številni standardi, npr. splošno uveljavljena standarda obvladovanja varovanja informacij ISO/IEC 27001 [1] in obvladovanja neprekinjenega poslovanja ISO 22301 [3], zato posebno pozornost posvečajo delu z zaposlenimi, njihovemu ozaveščanju in tudi nadzoru.

V magistrski nalogi smo s pomočjo raziskave predstavili učinek in pomen ozaveščanja zaposlenih pri vzpostavljanju in izvajanju varovanja informacij tako na področju dela v organizaciji kot v domačem okolju.

Ob uporabi analitične raziskave smo poskušali ugotoviti delež človeškega dejavnika in pokazati, da so ozaveščanje, izobraževanje in delo z zaposlenimi na splošno ključnega pomena pri zagotavljanju informacijske varnosti. Udejanjenje omenjenih priporočil v organizaciji lahko v praksi doprinese k vrsti dodatnih izboljšav na področju informacijske varnosti tako ključnih procesov kot drugih obsežnejših nalog in projektov.

Ugotovili smo, da je človeški dejavnik ključen za zagotavljanje varovanja informacij, a je v slovenskih organizacijah slabo poučen o aktualnih grožnjah, zato je za organizacije priporočljiva izvedba ustreznih izobraževanj oz. ozaveščanj.

Ključne besede:

varovanje informacij, informacijska varnost, človeški dejavnik, ISO/IEC 27001, ocena tveganj, informacijska tehnologija

Abstract

Increasing significance of information security is dictated primarily by technological advancement. Technical or IT solutions help greatly to increase key parameters of information security — confidentiality, integrity and availability. But this same technological advancement can often result in another factor being neglected — the human factor. Even if we secure information using IT solutions, it is installed, configured and maintained by — people. Numerous standards such as established ISO/IEC 27000 series for Information Security Management and ISO 22301 for Business Continuity Management focus increasingly on education and control of employees.

This thesis will demonstrate the importance and effect of employees' awareness in terms of establishing and maintaining information security at the workplace as well as in private environments. A social engineering experiment will serve to show the current state of information security awareness in several Slovenian organizations. Interviews will further demonstrate if any policies are in place and are being followed within these organizations. Furthermore, we will try to measure the effect an awareness workshop can have on increasing information security of key processes and other projects within an organization.

And finally, a theoretical risk analysis will serve to demonstrate the weight of human factor regarding threats and vulnerabilities present in an organizational environment.

We have found out that human factor is the key to ensuring an acceptable level of information security, but that employees in several Slovenian organizations are not sufficiently trained in information security. Therefore, it would be recommended to educate them properly and improve their awareness of the subject.

Razlaga pojmov in kratic

ISO — International Organization for Standardization

SUVI — Sistem upravljanja varovanja informacij

ISA — Information Security Awareness (ozaveščanje na področju varovanja informacij)

IT — Information Technology: informacijska tehnologija (tudi IKT — informacijsko-komunikacijska tehnologija)

SBR — Silver Bullet Risk: lastno razvito orodje za upravljanje s tveganji

PVI — politika varovanja informacij

OVI — ozaveščenost o varovanju informacij

1 Uvod

Naložbe v informacijsko-komunikacijsko tehnologijo (IKT) se osredotočajo pretežno na vlaganje v infrastrukturo, strojno opremo in naprave, komunikacijske rešitve, programsko opremo in storitve, povezane z IT. Pod pojmom IKT pravzaprav razumemo vsa našteta področja. Pogosto lahko posamezni organizaciji (ali pa celotni panogi) vlaganje v IKT prinese tržno prednost oz. sploh omogoči udejstvovanje v konkurenčnih dejavnostih.

Tudi upravljanje z IKT je v številnih organizacijah dobro podprto s pomočjo nabora dobrih praks in sistemov vodenja, kot so Cobit, ITIL in sorodni. Zavedanje, da uporaba tehnologije prinaša določeno stopnjo tveganja, je v organizacijah precej močno zasidrano. Tveganje v razvitih organizacijah predstavlja dejavnik, ki ga je prav tako treba obvladovati — od stroškov vpeljave neke tehnologije do optimizacije in zagotavljanja njenega nemotenega delovanja, kot tudi njene varne rabe. Pod pojmom varnosti v svetu informatike obravnavamo predvsem tri ključne vidike: varovanje zaupnosti, razpoložljivosti in celovitosti (integritete) posameznih podatkov, informacij, informacijskih sistemov in celotnih tehnologij [1].

S sistematičnim pristopom k varovanju informacij se je v zadnjem desetletju uveljavila vrsta sistemov vodenja (angl. management systems) z večjim poudarkom na varovanju teh ključnih in tudi drugih meril ter obenem obvladovanju povezanih tveganj. Na evropskem področju se je uveljavil predvsem sistem upravljanja varovanja informacij britanske organizacije BSi (British Standards Institute), ki ga je nadgradila mednarodna organizacija za standardizacijo ISO pod skupino standardov serije ISO/IEC 27001 [1].

1.1 Opredelitev problema

Temeljno izhodišče varovanja informacij je običajno skrb zanje ne glede na njihovo obliko. Lahko so torej informacije, shranjene v podatkovnih zbirkah, datoteke programov, torej informacije, ki nastanejo in "živijo" v digitalnem svetu, informacije, ki se prenašajo po komunikacijskih poteh, kot tudi informacije, ki jih imamo zapisane ali natisnjene na papirju, in neoprijemljive informacije, ki so lahko bolj ali manj verodostojno shranjene v človeškem spominu, v to skupino pa uvrščamo tudi npr. ugled podjetja. Določen podatek oz. informacija lahko za organizacijo predstavlja neko vrednost, neodvisno od medija hrambe.

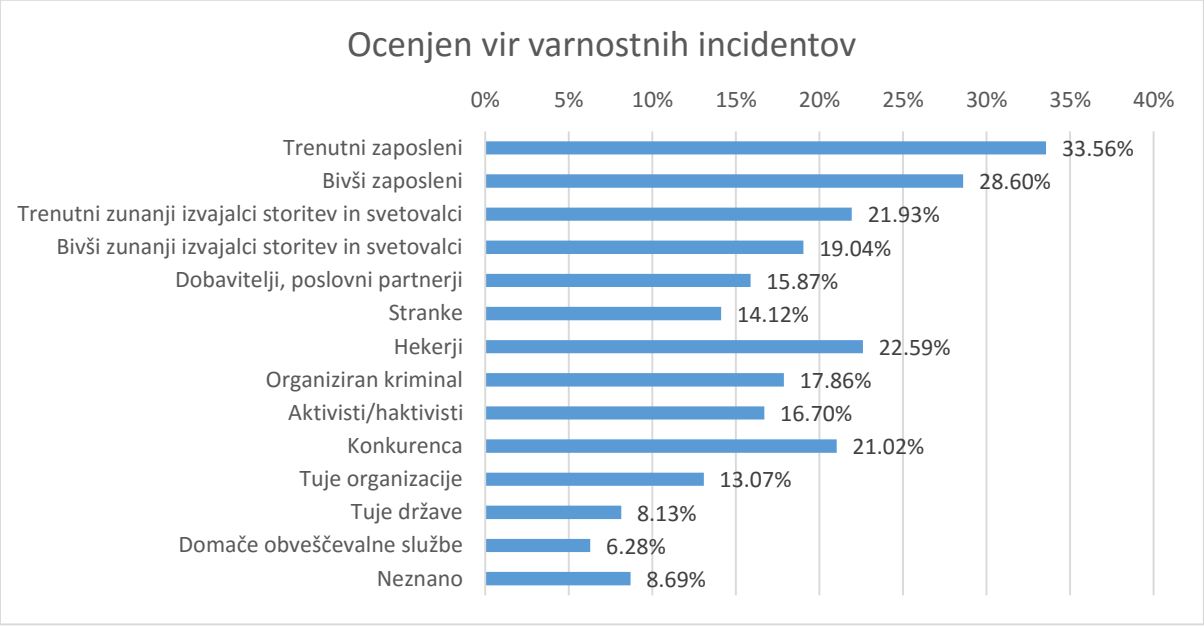
Ob pospešenem tempu digitalizacije podatkov in informacij ter spreminjanju procesov organizacij, ki to digitalizacijo s pridom izkoriščajo, organizacije že desetletja večajo učinkovitost teh procesov in svojo konkurenčno prednost. Ob tem se zavedajo, da

informacije oz. informacijski tokovi predstavljajo bistvo večine njihovih procesov, saj se ti brez informacij in pretoka ne bi mogli izvajati.

Smiselnost vlaganj v informatizacijo torej ni pod vprašajem, večji pomen pa ima zato vprašanje, kako zagotoviti učinkovitost teh vlaganj, jih uskladiti s poslovnimi cilji in zagotoviti čim večjo donosnost (ROI oz. Return-on-Investment).

Pogosto pa se ob vlaganjih v tehnologijo zanemari drug dejavnik — dejavnik ljudi, ki morajo to tehnologijo premišljeno izbrati, jo umestiti v poslovno okolje, z njo vsak dan delati in upravljati ter jo ob koncu njene življenjske dobe tudi učinkovito odstraniti oz. nadomestiti. Zanemarjanje človeškega dejavnika je lahko zelo očitno — vodstvo podjetja se npr. odloči za nakup poslovne programske opreme, ne upoštevajoč, da bodo imeli zaposleni ogromne težave s prehodom na nov način dela oz. z njegovim učenjem. Lahko pa je premajhen poudarek na človeškem dejavniku precej bolj prikrit — zaposlene lahko naučimo delati z novo tehnologijo, njihove postopke natančno dokumentiramo in predpišemo ter nadziramo, pozabimo pa, da lahko že majhna nenamerna napaka pri vnosu nekega podatka uniči celovitost podatkovne baze.

Analiza svetovne revizijske družbe PricewaterhouseCoopers (PwC) za leto 2015 [11] med najpogostejšimi viri incidentov navaja zaposlene in bivše zaposlene v organizaciji.



Slika 1: Ocenjen vir varnostnih incidentov [11]

Stroka torej pogosto namenja nesorazmerno veliko sredstev tehničnim rešitvam za zagotavljanje varovanja informacij [8] v primerjavi z vlaganji v ozaveščanje in izobraževanje zaposlenih. Njihova odgovornost je pogosto opredeljena v politikah in pravilnikih, katerih

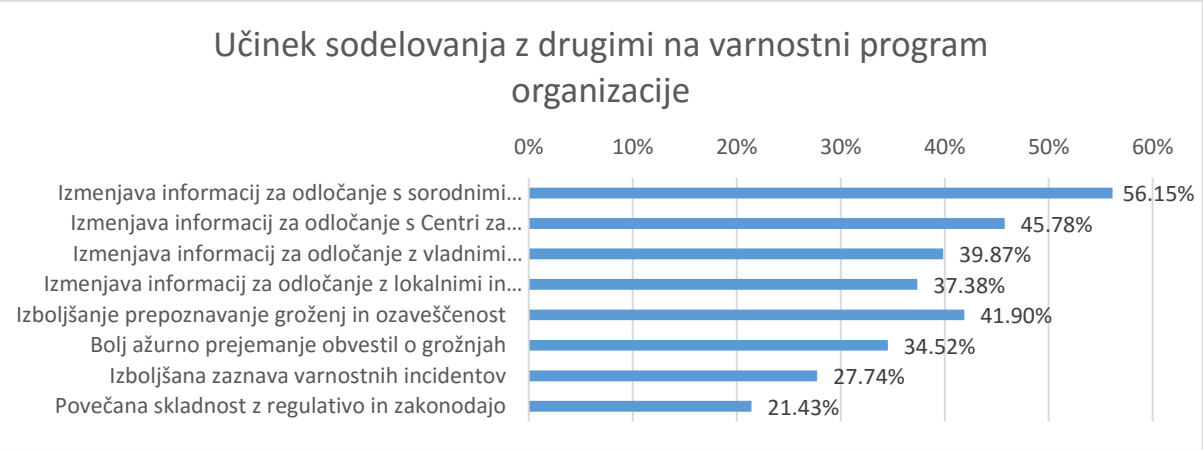
izvajanje se preverja le ob varnostnih presojah, zanemarja pa se vzpostavitev kulture varovanja informacij v vsakodnevnem izvajanju dejavnosti oz. organizacijskih procesov.

1.2 Namen in cilji magistrske naloge

Pričakovan rezultat magistrske naloge je ocena pomembnosti ozaveščenosti ljudi (zaposlenih) o potencialnih nevarnostih oz. incidentih, ki pretijo njihovi organizaciji, domačemu okolju ali širši družbi. Za dosego rezultata bo uporabljena analiza rezultatov raziskav in izvedena ocena tveganja. S pomočjo ugotovljenega deleža, ki ga v obravnavi varovanja informacij predstavlja človeški dejavnik, bomo pokazali, da so ozaveščanje, izobraževanje in delo z zaposlenimi na splošno ključnega pomena pri zagotavljanju informacijske varnosti v smislu preprečevanja številnih ranljivosti, ki smo jim vsakodnevno izpostavljeni in jih je mogoče s pomočjo družbenega inženiringa in drugih groženj precej preprosto izkoristiti.

Udejanjenje omenjenih priporočil v organizaciji lahko v praksi doprinese k vrsti dodatnih izboljšav na področju informacijske varnosti tako ključnih procesov kot drugih obsežnejših nalog in projektov.

Slednje potrjujejo tudi izsledki raziskave že omenjene PwC [11], ki poleg izmenjave podatkov s sorodnimi organizacijami v panogi in temu namenjenimi podjetji na tretje mesto uvršča prepoznavanje groženj in ozaveščanje kot ključna vpliva na programe informacijske varnosti.



Slika 2: Vpliv sodelovanja z drugimi na varnostni program organizacije [11]

1.3 Metodologija

Za opredelitev pomena človeškega dejavnika problematike varovanja informacij smo poskušali ta dejavnik izraziti kvalitativno in kvantitativno ter s tem dokazati in poudariti njegovo ključno vlogo pri zagotavljanju varnega delovanja.

Ugotavljanja deleža in vpliva človeškega dejavnika glede varovanja informacij smo se lotili na tri načine:

1. kvantitativna ocena tveganja s pomočjo orodja bo namenjena identificiranju s človeškim dejavnikom povezanih groženj in ranljivosti prisotnih v primeru organizacijskega okolja;
2. splošna identifikacija razširjenosti problematike s pomočjo poskusa družbenega inženiringa na psevdonaključnem vzorcu 85 organizacij v osrednjeslovenski regiji;
3. analiza učinka delavnic ozaveščanja v konkretni organizaciji s pomočjo vprašalnikov pred in po delavnici ozaveščanja.

Vsak izmed treh pristopov nudi svojevrsten vpogled v dinamiko varovanja informacij s poudarkom na mogočih zlorabah, katerih vir je lahko človeški dejavnik.

Podrobnosti posameznega pristopa bodo opisane v nadaljevanju.

2 Varovanje informacij in človeški dejavnik

2.1 Teorija varovanja informacij

Potreba po varovanju informacij izhaja že iz časa pred njihovim pojavljanjem v digitalni obliki. Že pred našim štetjem so vojaški vodje razumeli pomen ščitenja zaupnosti ključne korespondence in so začeli uporabljati mehanizme, ki so informacije ščitili tako fizično (zaklenjene škatle) kot tudi pomensko (preprosti šifrirni algoritmi).

V 19. stoletju so se razvili kompleksnejši sistemi klasifikacije, ki so vladam omogočili upravljanje informacij glede na stopnjo zaupnosti in posebno obravnavo v temu namenjenih institucijah.

Različni standardi oz. viri navajajo različne definicije, kaj natančno je varovanje informacij. Skupno večini pa je, da obravnavajo tri ključna merila: zaupnost (ang. confidentiality), celovitost (ang. integrity) in razpoložljivost (ang. availability) informacije. Nabori relevantnih ciljev, ki jih zasleduje področje varovanja informacij, lahko poleg omenjenih treh kategorij vključujejo še zasebnost (ang. privacy), avtentičnost (ang. authenticity), zaupanja vrednost (ang. trustworthiness), nezatajljivost (ang. non-repudiation), odgovornost (ang. accountability) in presojevalnost (ang. auditability).

Danes za mnogo ali kar večino organizacij predstavljajo informacije in tehnologija, ki jih podpira, eno najpomembnejših sredstev oz. virov. Uspešna podjetja se tega zavedajo, zato s pridom izkoriščajo vse prednosti, ki jih informatizacija prinaša, ter tako dvigujejo lastno vrednost in zvišujejo konkurenčno prednost.

Da lahko tako podjetje zagotovi obstoj te informacijske prednosti, mora z informacijami pravilno ravnati in jih načrtno upravljati. Med ključne procese upravljanja informacij spada tudi ocenjevanje tveganja. Ta proces se poleg finančnih in drugih vidikov osredotoča predvsem na področje informacijske varnosti, ki je zadnja leta pereč problem vseh informacijskih sistemov.

2.2 Pregled dobrih praks

V številnih gospodarskih segmentih se dobre prakse odražajo v obliki standardov, ki jih organizacije vpeljejo z namenom celostnega pokrivanja ali izboljšanja posameznega področja delovanja oz. organizacijskega procesa. Standardi lahko zagotovijo oz. omogočijo varnost, zanesljivost, skladnost z zakonodajo in regulatornimi zahtevami, interoperabilnost

ter številne poslovne prednosti (dostop do tržišč, ekonomija velikih količin, spodbujanje inovativnosti, povečana ozaveščenost).

Tudi na področju varovanja informacij organizacije dobre prakse najpogosteje udejanjijo v obliki standardov, ki jih vpeljejo v svojo združbo (v organizacijo samo in v sodelovanje z zunanjimi deležniki).

Standard **ISO/IEC 27001** [1] se je tako v zadnjem desetletju, sploh v Evropi, uveljavil kot najprepoznavnejše ogrodje za sistematično gradnjo sistema upravljanja varovanja informacij. Ker svojo skladnost s standardom organizacija lahko izkazuje s pomočjo certificiranja, se marsikatera ponaša z oznako *"ISO/IEC 27001 certified"*, kar ji prinese določeno mero ugleda in zaupanja vseh deležnikov (strank, partnerjev itd.).

Standard je prilagojen različnim velikostim in tipom organizacij, saj predstavlja le okvir oz. ogrodje, za implementacijo pa mora običajno organizacija poskrbeti sama in jo prilagoditi lastnim potrebam in kontekstu poslovanja.

Ključni element je kontinuirana obravnava vseh dejavnikov, povezanih z varovanjem informacij. Vseh sprememb oz. izboljšav naj bi se organizacija lotila po klasičnem ciklu PDCA (angl. Plan-Do-Check-Act), z namenom preučiti mogoče ovire in pripraviti potrebne vire ter slediti vpeljavi in uspešnosti posameznih izboljšav.

Del standarda je tudi sistematična obravnava tveganj ter z njimi povezanih groženj in ranljivosti. Metodologija ni predpisana, priporoča pa se uporaba relativno preproste metode s pomočjo matrik tveganj, kjer se tveganje določi iz matrike ob določanju stopnje pojavnosti (frekvence) groženj oz. ranljivosti in njihovega vpliva.

Standard naborov groženj oz. ranljivosti ne navaja, ampak to prepušča organizacijam.

ISO 27001 številna poglavja in povezane kontrole namenja prav upravljanju človeških virov v povezavi z upravljanjem varovanja informacij. Postopek zaposlitve, izvajanje delovnih nalog, upravljanje z viri organizacije in druga poglavja so namenjena prenosu odgovornosti za varovanje informacij na posameznika. Standard zahteva vpeljavo kontrol, ki natančno opredeljujejo odgovornosti zaposlenih za varovanje informacij in vrsto drugih, z zaposlenimi povezanih kontrol, ki se tičejo postopkov pred zaposlitvijo, med njo in po njej. Incidente, povezane s človeškim dejavnikom, je mogoče kategorizirati na različne načine, od napak in nenamernih kršitev [4] do drugih dejanj z namenom okoriščanja ali povzročanja negativnih posledic [5, 6].

COBIT 5 za varovanje informacij

Združenje ISACA je bilo ustanovljeno že leta 1969 z namenom povezati posameznike, ki so čutili potrebo po osrednjem viru informacij in smernicah na področju akreditacij računalniških oz. informacijskih sistemov. V skoraj petdesetih letih je združenje razvilo številne praktične smernice, merila in orodja za potrebe organizacij. Med najbolj znane se uvršča ogrodje COBIT, ki posebno področje namenja prav varovanju informacij — COBIT 5 for Information Security [12].

Pri tem ogrodju je človeški dejavnik obširno opredeljen v okviru upravljanja varovanja informacij v organizacijah. Izpostavlja tri ravni, ki se jih ne sme zanemariti: uprave v vodstveni vlogi, odgovorne za varovanje informacij, ki morajo izvajati varnostne strategije, in končne uporabnike, ki morajo biti aktivno soudeleženi v procesu varovanja informacij. Glede na COBIT lahko organizacija gradi odpornost s preprečevanjem varnostnih incidentov, njihovim zaznavanjem in okrevanjem po varnostnih incidentih le, če vse tri ravni prevzamejo svoj delež odgovornosti [13].

PCI DSS

PCI Security Standards Council (oz. Svet varnostnih standardov v industriji plačilnih kartic) je svoj vpliv razširil z relativno ozkega področja presoj varnosti POS-terminalov in drugih tehnologij za varnost v kartičnem prometu na široko področje razvoja, izboljšave, hrambe, razširjanja in implementacije varnostnih standardov za varovanje računov, kartičnega poslovanja oz. osebnih podatkov strank. Standard obsega več kontrolnih seznamov (checklists) z namenom strukturiranega preverjanja skladnosti oz. ustreznosti posameznih elementov v informacijskih sistemih. Številne varovalke so namenjene prav zaščiti pred grožnjami, ki bi lahko izkoristile človeško neprevidnost. V ta namen navaja posebne dobre prakse za vpeljavo programa ozaveščanja [15].

ISF Standard of Good Practice for Information Security

ISF Standard [16] je bil razvit z namenom pokrivanja kar se da širokega spektra področij, povezanih z varovanjem informacij. Ob implementaciji naj bi pokril tako skladnost z ISO/IEC 27002:2013, Cobit 5 kot tudi SANS Top 20 in NIST Cyber Security Framework. Ključna področja, ki jih ISF pokriva, so dvig odpornosti pred spreminjajočim se obsegom groženj, skladnost s ključnimi standardi s področja varovanja informacij, preverjanje dogovorov o varovanju informacij z zunanjimi izvajalci, podlaga za analizo tveganja varovanja informacij, podlaga za politike, standarde in postopke, dvig ozaveščenosti o varovanju

informacij, podlaga za podrobno ali krovno oceno tveganja in razvoj ali izboljšave varovanja informacij v odgovoru na nove grožnje.

Ocenjevanje tveganj

Večina omenjenih standardov in dobrih praks kot najboljši način prilagoditve posamezni organizaciji vključujejo izdelavo ocene tveganj (angl. risk assessment), s pomočjo katere organizacija identificira največja tveganja in pripravi oz. vpelje ustrezne ukrepe, s katerimi ta tveganja zmanjša.

Analiza tveganj običajno obsega identifikacijo in vrednotenje dveh meril pri vsaki grožnji ali ranljivosti — verjetnosti udejanjenja neke grožnje (ali izkoriščenja ranljivosti) in posledice tega udejanjenja.

Vrednotenje tako verjetnosti kot posledic je pogosto težavno, obstajajo pa določeni modeli, ki nam vrednotenje olajšajo oz. približajo [7].

Številni avtorji so soglasni, da poenoten univerzalni pristop k varovanju informacij ni mogoč, ampak mora biti prilagojen posameznemu okolju oz. naravi organizacije. V določenih strukturah je mogoče zelo podrobno formalizirati postopke in odgovornosti, v manjših okoljih pa bi to privedlo do prevelike rigidnosti, zato je tu še posebnega pomena osnovno ozaveščanje uporabnikov, ki tako spoznajo in v prihodnje prepoznajo potencialne izvore incidentov in se naučijo primernega ukrepanja.

Varnostne politike

Varnostne politike so temeljni dokument, s katerim organizacija nek ukrep vpelje v svoje poslovno okolje. Namen politike je zaposlenim sporočiti podlago za neko odločitev, jo natančno definirati in od vseh zahtevati skladno delovanje ter po potrebi določiti sankcije v primeru neskladnega ravnanja.

Šele s pomočjo tovrstne formalizacije lahko vodstvo organizacije pričakuje, da bodo zaposleni ravnali zahtevam primerno, v nasprotnem primeru so lahko marsikatere aktivnosti oz. podrobnosti izvedbe posameznih procesov prepuščene izključno dosedanjim izkušnjam zaposlenih.

Prav tako mora politika odražati zahteve veljavne zakonodaje, npr. o varstvu osebnih podatkov. Le z vnaprej opredeljenim načinom dela, s katerim so seznanjeni zaposleni, lahko organizacija uveljavi določene pravice, npr. vpogleda v opremo, ki je sicer last organizacije, a jo uporablja posameznik in bi zato lahko pri posegu nehote kršila pravico do zasebnosti.

Šele ko je vnaprej opredeljeno, da se na določeni opremi lahko hrani le določena poslovna vsebina, lahko organizacija izvede tak poseg.

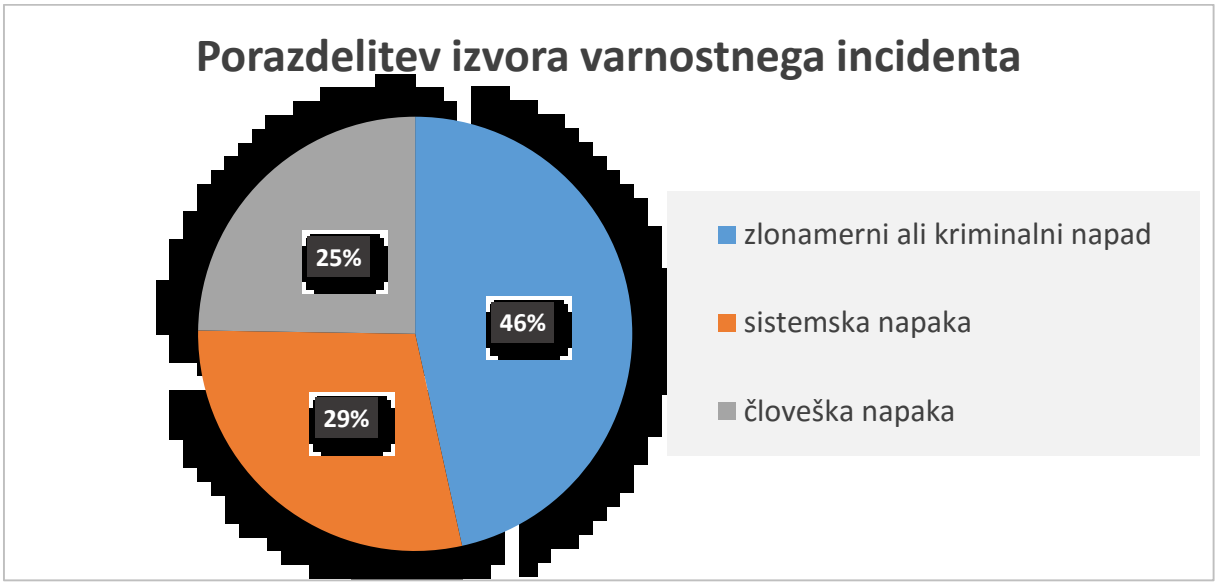
2.3 Trendi zlorab informacijske varnosti

Analize na svetovni ravni

Številne organizacije izvajajo kvantitativne raziskave incidentov, povezanih z varovanjem informacij. Rezultati so različni, ker lahko zajemajo le posamezno državo, gospodarski segment ali velikost organizacij.

Revizijska hiša PricewaterhouseCoopers izvaja globalne raziskave [11] in je v letu 2015 zaznala porast števila zaznanih incidentov v višini 38 % v primerjavi z letom 2014. V smislu posledic je zabeležila porast primerov kraje intelektualne lastnine kar za 56 %. Se pa je v letu 2015 za 5 % zmanjšala količina finančnih izgub zaradi incidentov v primerjavi z letom 2014. Glede na vpeljane varnostne mehanizme 53 % organizacij izvaja izobraževanja zaposlenih in programe ozaveščanja na področju informacijske varnosti.

Zanimiva je tudi raziskava družbe Ponemon za leto 2015 [9], katere naročnik je družba IBM. Preučevanje stroškov incidentov, povezanih s podatki, že daje delno sliko o pomenu človeškega dejavnika pri zagotavljanju varovanja informacij.

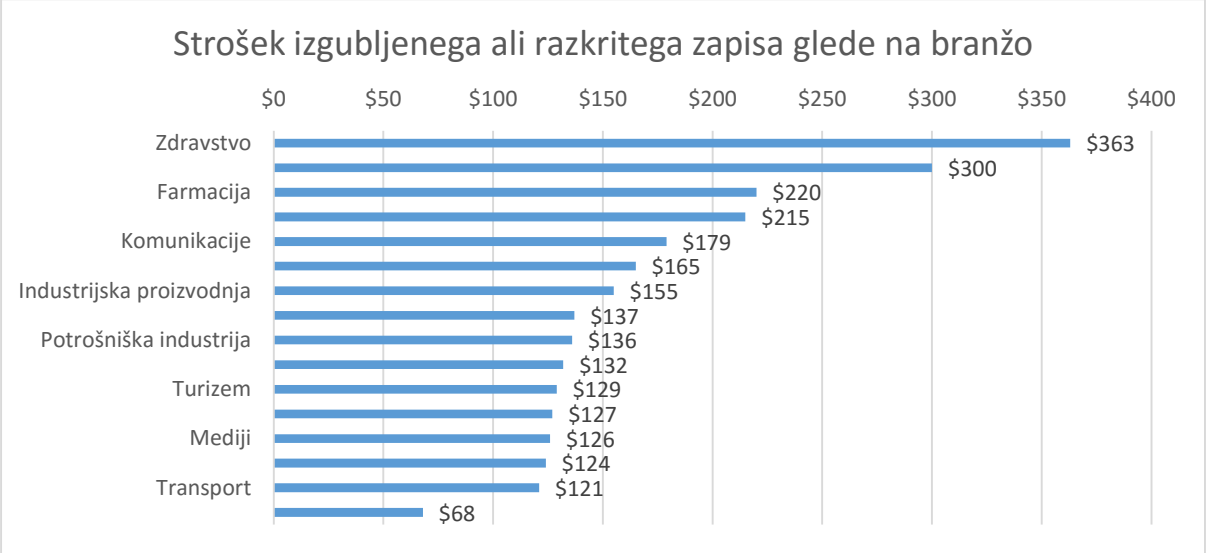


Slika 3: Izvor varnostnih incidentov v vzorcu (n = 350) [9]

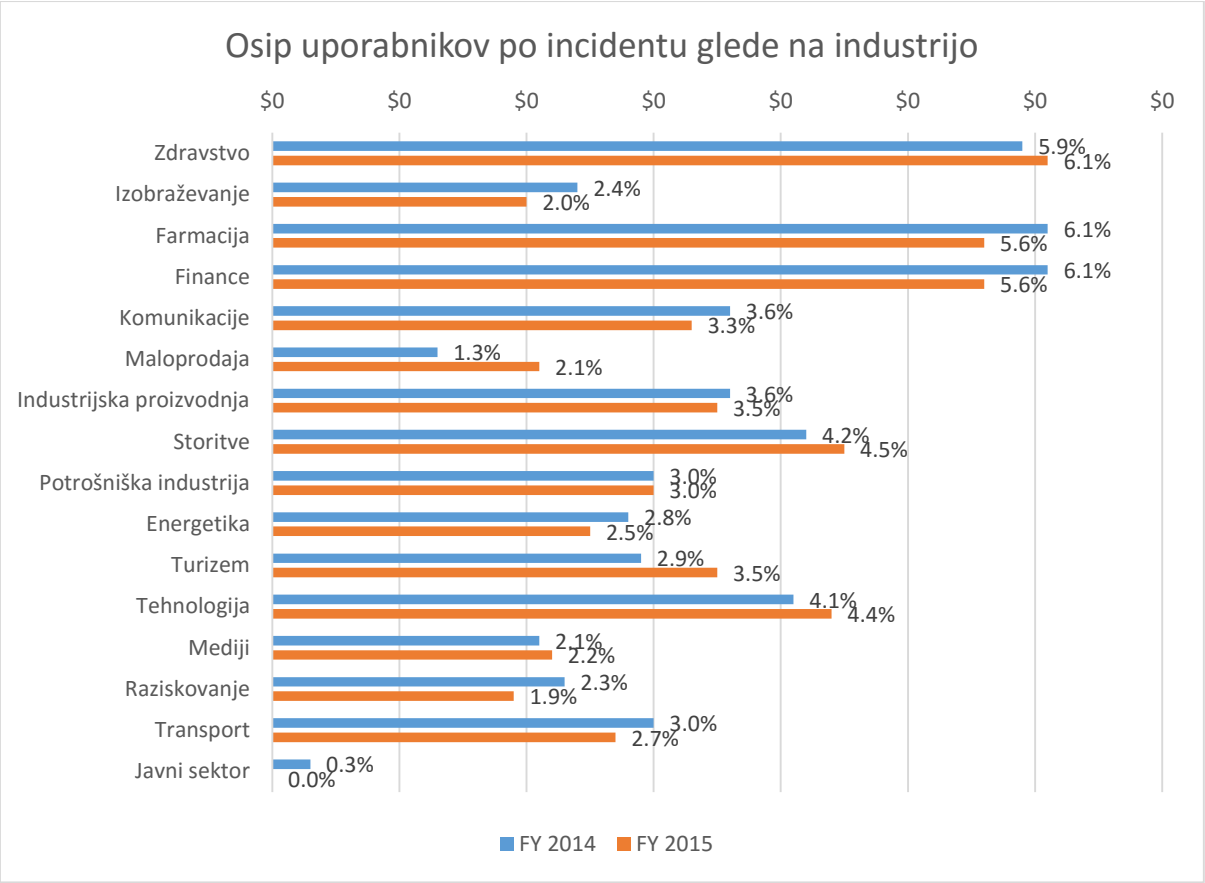
Neposredna človeška napaka je po izsledkih raziskave vir razkritja zaupnih podatkov v 25 % primerov. Če upoštevamo, da je tudi za sistemske napake in zlonamerne napade v določenem

odstotku (so)kriv notranji človeški dejavnik, npr. če je bil podvržen družbenemu inženiringu ali izsiljevanju, je lahko krivda človeškega dejavnika še toliko večja.

Zdravstveni sektor je še posebej izpostavljen kot najranljivejši — tako glede stroškov izgubljenega oz. razkritega zapisa kot tudi zaradi največjega osipa uporabnikov po incidentu (angl. churn rate).



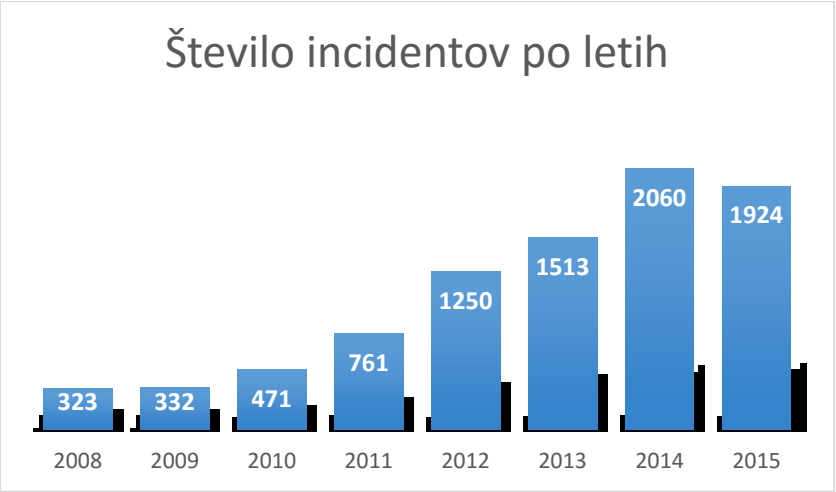
Slika 4: Cena izgubljenega oz. razkritega zapisa [9]



Slika 5: Osip uporabnikov po incidentu [9]

Analize v Sloveniji — poročilo SI-CERT

V Sloveniji tovrstne analize izvaja skupina SI-CERT, ki deluje v okviru akademske raziskovalne mreže Arnes. Dogodke uvrstijo v tri kategorije: tehnični napadi, goljufije in prevare ter poizvedbe. Najzgovornejši je graf letnega porasta števila obravnavanih incidentov. V letu 2015 je SI-CERT prvič zabeležil rahel upad števila incidentov, predvsem zaradi upada tehničnih napadov, ki jih je po številu prvič prehitela kategorija goljufij in prevar, kjer je oškodovanec predvsem določena oseba in ne informacijski sistem.



Slika 6: Trend naraščanja obravnavanih incidentov v Sloveniji [5]

Tudi za pojave škodljive kode, ki so sicer uvrščeni pod tehnične napade, je v veliki meri odgovoren človeški dejavnik zaradi nevednosti oz. neprevidnosti.

Statistika obravnavanih incidentov								
Vrsta incidenta	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
Skeniranje in poskušanje	86	39	44	62	51	43	65	65
Botnet	9	3	11	12	12	16	13	17
Napad onemogočanja (DDoS)	22	10	18	28	47	76	124	94
Škodljiva koda	18	53	68	126	258	417	438	418
Zloraba storitve	16	15	12	28	9	8	9	15
Vdor v sistem	32	25	56	93	76	61	32	43
Zloraba up. računa				1	9	37	60	40
Razobličenje					125	80	167	33
Napad na aplikacijo					17	22	33	7
Tehnični napadi skupaj	**183**	**145**	**209**	**350**	**604**	**760**	**941**	**732**
Kraja identitete			10	52	67	56	77	70
Nigerijska (419) prevara							38	26
Spletno nakupovanje							68	88
Druge goljufije	5	24	26	89	161	210	309	322
Spam	21	22	36	25	74	50	63	112
Phishing	23	38	50	61	139	209	279	83
Dialler					1		3	
Goljufije in prevare skupaj	**49**	**84**	**122**	**227**	**442**	**525**	**837**	**901**

Slika 7: Vrste incidentov v Sloveniji po letih [5]

Arnes mnogo prizadevanj vlaga v ozaveščanje javnosti preko projektov, kot sta “Varni na internetu” in “Safe.si”. Tudi skupina Safe Mode, katere vodja je avtor naloge, sodeluje z Arnesom pri določenih projektih.

2.4 Obvladovanje tveganj

Da lahko tako podjetje zagotovi obstojnost informacijske prednosti, mora z informacijami pravilno ravnati, jih upravljati. Med ključne procese upravljanja informacij spada tudi ocenjevanje tveganja. Ta proces se poleg finančnih in drugih vidikov poslovanja osredotoča predvsem na področje informacijske varnosti, ki je zadnja leta pereč problem vseh informacijskih sistemov.

Čedalje pogostejši so namreč primeri izgub, kraj, vdorov ali drugih načinov zlorabe informacij, zato mnoga podjetja veliko sredstev usmerjajo prav v problematiko analize, upravljanja in zagotavljanja informacijske varnosti.

Vsa priporočila, dobre prakse, standardi in zakonodajne zahteve kot osnovni pokazatelj stanja trenutne stopnje informacijske varnosti in smernice za njeno izboljšanje izrazijo potrebo po implementaciji in izvedbi postopka **ocenjevanja in upravljanja tveganja informacijske varnosti**. Postopek mora biti del načrtovalne oz. organizacijske faze implementacije sistema, saj le tako lahko zagotovimo učinkovito izrabo sredstev.

Postopka se različne metodologije lotevajo različno, odvisno od potreb organizacije po skladnosti z različnimi standardi oz. zakonodajnimi zahtevami.

Po COBIT-u lahko tveganje IT opredelimo kot poslovno tveganje, ki je povezano z uporabo, lastništvom, izvajanjem, vključevanjem, vplivanjem in vpeljavo informacijske tehnologije znotraj organizacije. V ta namen določa smernice, kaj je potrebno za vzpostavitev in izvedbo učinkovite in uspešne funkcije obvladovanja tveganj.

COBIT tudi našteje ključna gonila za upravljanje tveganj [18]:

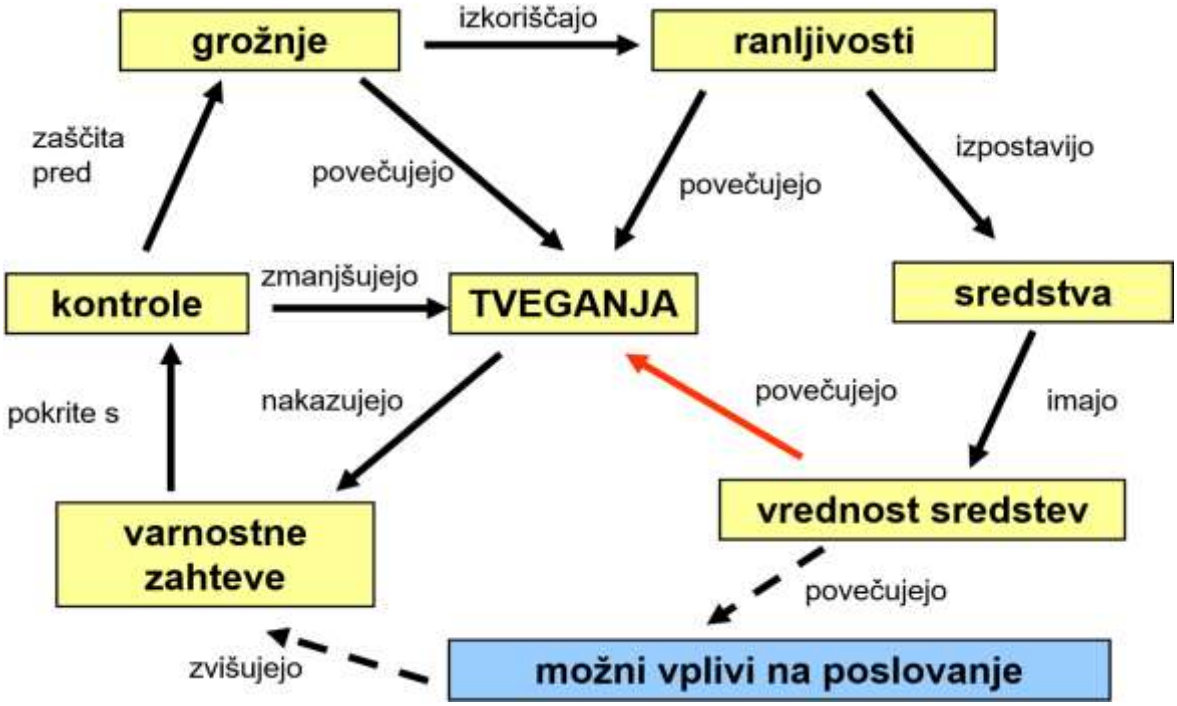
- opredeljen in konsistenten pregled stanja tveganj v organizaciji za vse njene deležnike,
- vodenje upravljanja tveganj do ravni, ki je znotraj sprejemljive stopnje tveganj (angl. risk appetite) organizacije,
- vodenje k vzpostavitvi primerne kulture tveganja v organizaciji,
- kvantitativna ocena tveganja omogoča deležnikom upoštevati stroške zmanjševanja tveganj in potrebnih virov v primerjavi z izpostavljenimi izgubami.

Predvsem na zadnje izmed naštetih gonil se naslanja tudi model analize tveganja, ki ga bomo uporabili za študijo primera in potrjevanje izhodiščne trditve v nadaljevanju (poglavje 3.1).

Ocenjevanje tveganja informacijske varnosti, kot ga definira ISO 27001, je »ocena groženj, ki pretijo informacijskim sredstvom, možnosti njihove pojavitve, učinkov teh groženj na sredstva in ranljivosti informacij in informacijskih sredstev« [1, 2]. Seveda se standard pri definiciji **informacijskih sredstev** ne omejuje zgolj na programsko in strojno opremo, temveč obsega tudi informacije v papirni obliki, znanje in izkušnje zaposlenih, komunikacije preko nedigitalnih medijev itd. ISO 27001 jih zato privzeto razdeli v naslednje skupine:

- okolje in infrastruktura (npr. pisarna, električni vodniki itd.),
- osebje (npr. zaposleni, stranke),
- strojna oprema (npr. delovne postaje, strežniki),
- programska oprema (npr. aplikacije, operacijski sistemi),
- komunikacije in komunikacijska oprema (npr. usmerjevalniki, optični kabli),
- dokumenti in podatki (v digitalni in nedigitalni obliki),
- ostala sredstva informacijske narave (npr. ugled podjetja).

Slika 8 nazorno prikaže, kakšen medsebojni vpliv imajo posamezni parametri tveganja.



Slika 8: Model medsebojne odvisnosti parametrov tveganja

Hitro lahko opazimo, da je vpeljava **varnostnih kontrol** ključni dejavnik za zmanjševanje tveganj. Vse metodologije ocenjevanja tveganja zato vnaprej predvidijo določen nabor teh kontrol, ki pa seveda ni zaključen in ga lahko podjetje po izvedeni oceni tveganja razširi s

poljubnimi kontrolami, ki jih metodologija (še) ne vsebuje ali pa so preveč posebne, vendar še vedno potrebne.

Grožnje, ki pretijo informacijskim sredstvom, so odvisne od tipa sredstva. Tipičen primer grožnje je npr. »odpoved električnega napajanja«, ki izkorišča ranljivost »nestabilne preskrbe z električno energijo« informacijskega sredstva, »delovna postaja Max3«. Nezaželena lastnost sredstev so namreč **ranljivosti**, ki se jim pogosto žal ne moremo izogniti, če želimo, da sredstvo opravlja neko nalogo. Verjetnost, da bo neka grožnja neko ranljivost izkoristila, predstavlja osnovno merilo pri ocenjevanju tveganja za določeno informacijsko sredstvo. Med primere ranljivosti lahko uvrstimo npr. nezadostno kontrolo dostopa, pomanjkljive varnostne politike, nezaščitena gesla itd. [5].

Opredelimo še pojem **vrednost informacijskih sredstev**. Ta ni izražena le finančno, temveč vsebuje tudi parametre zaupnosti, celovitosti in razpoložljivosti. Za primer poglejmo nek zapis v bazi strank. Ta s stališča finančne vrednosti ne predstavlja nujno visokega zneska, vendar pa je za nas lahko mnogo pomembneje, da podatek o tej stranki ne pride v javnost, zato je tveganje pred izgubo zaupnosti lahko zelo pomemben dejavnik in ga moramo v največji meri minimizirati.

2.5 Človeški dejavnik pri varovanju informacij

Človeški dejavnik smo delno že izpostavili, predvsem pri pregledu dobrih praks. Znotraj organizacijskega okolja je lahko ta pojem zelo široko opredeljen, saj lahko skoraj vsak dogodek ali dejanje (razen npr. naravne nesreče) povežemo s človeškim dejavnikom. Še ko gre primarno za tehnični incident, npr. pri vdoru v strežnik, je človek tisti, ki je strežnik konfiguriral, vzdrževal. Za incidente, ki izhajajo izven organizacije, pa je prav tako v večini primerov odgovoren človek — storilec.

Kljub tovrstnim povezavam, ki še dodatno širijo vpliv človeškega dejavnika, se bomo v njegovi obravnavi poskušali omejiti na bolj neposreden pogled, torej predvsem na vidik končnega uporabnika.

Dejanja zaposlenih lahko narekujejo njihova motivacija za delo, osebni vzgibi in želje, njihovo znanje in izkušnje in predvsem zahteve organizacije. Te zahteve določajo, kaj, kako in kdaj mora biti posamezna dejavnost izvedena. Pri varovanju informacij so določila podana v obliki operativnih postopkov, predpisov, politik ali zakonov.

Ni pa dovolj, da ta določila samo obstajajo, zaposlenim morajo biti ustrezno sporočena, razumljiva, razumeti morajo razlog za njihov obstoj in posledice (ne)skladnega ravnanja. To

ugotavlja Stanton [17], ki dodaja, da če zaposleni niso motivirani za izvajanje dejavnosti, potrebnih za zaščito informacij in tehnoloških virov organizacije, se politike ne preslikajo v zaželeno obnašanje.

Ozaveščenost uporabnika predstavlja pomembno merilo za učinkovitost varovanja informacij v organizaciji. Ozaveščenost lahko opredelimo kot splošno znanje o varovanju informacij in poznavanje določil in dejanske prakse organizacije.

Področje učinka politik, se pravi izida ravnanja zaposlenih, ki je lahko skladno ali neskladno z določili, je predmet raziskave [8], ki je s pomočjo kompleksnega ogrodja potrdila vrsto hipotez (neposredno povzeto in prevedeno):

- Hipoteza 1: Odnos zaposlenega do skladnosti s PVI pozitivno učinkuje na namero skladnega ravnanja s PVI.
- Hipoteza 2: Izhodiščno prepričanje zaposlenega o skladnosti s PVI organizacije pozitivno učinkuje na namero ravnanja skladno s PVI.
- Hipoteza 3: Samoučinkovitost zaposlenega v skladnem ravnanju s PVI pozitivno učinkuje na namero ravnanja, skladnega s PVI.
- Hipoteza 4a: Notranja dobrobit, ki jo zaposleni pridobi ob ravnanju, skladnem s PVI, je sorazmerna z zaznano prednostjo skladnosti.
- Hipoteza 4b: Varovanje virov organizacije, ki izhaja iz ravnanja zaposlenega, skladnega s PVI, je sorazmerno z zaznano prednostjo skladnosti.
- Hipoteza 4c: Nagrada, ki jo je deležen zaposleni za ravnanje skladno s PVI, je sorazmerna z zaznano prednostjo skladnosti.
- Hipoteza 5: Ovira pri delu zaposlenega zaradi skladnosti s PVI je sorazmerna z zaznano ceno skladnosti.
- Hipoteza 6a: Notranji strošek, ki doleti zaposlenega kot posledica neskladnosti s PVI, je sorazmeren z zaznanim stroškom neskladnosti.
- Hipoteza 6b: Ranljivost organizacijskih virov, ki je rezultat neskladnosti zaposlenega s PVI, je sorazmerna z zaznanim stroškom neskladnosti.
- Hipoteza 6c: Sankcije, ki jih je lahko deležen zaposleni zaradi neskladnosti s PVI, so sorazmerne z zaznanim stroškom neskladnosti.
- Hipoteze 7a/7b/7c: OVI zaposlenega je sorazmerna z notranjo dobrobitjo (a)/varovanjem virov (b)/nagrado (c).
- Hipoteza 8: OVI zaposlenega je obratno sorazmerna z oviro pri delu.
- Hipoteze 9a/9b/9c: OVI zaposlenega je sorazmerna z notranjim stroškom (a)/ranljivostjo virov (b)/sankcijami (c).

Navedene hipoteze nam pomagajo definirati ključna merila, ki vplivajo na ozaveščenost zaposlenih glede varovanja informacij. Ta merila bomo vrednotili tudi v naših analizah človeškega dejavnika (s pomočjo poskusa družbenega inženiringa, raziskave s pomočjo vprašalnikov in kvantitativne analize tveganja).

Tudi slovenska raziskava je potrdila korelacijo med znanjem oz. ozaveščenostjo in pozitivno povezavo z varno uporabo IKT — višja kot je stopnja znanja, pogostejše je tudi dejansko varno vedenje pri uporabi IKT v podjetjih oz. tisti z več znanja se tudi pri uporabi računalnika vedejo manj tvegano [20].

2.6 Človeški dejavnik pri informacijskih zlorabah

Primeri zlorab informacij, povezanih s človeškim dejavnikom, navadno vključujejo naslednje družbene elemente: neznanje, prenizko ozaveščenost, nerodnost (nagnjenost k napakam), »čredni nagon«, kot tudi pozitivne osebnostne lastnosti, kot so zaupljivost, ustrežljivost, pripravljenost pomagati, ubogljivost. Pogosto se v teh primerih družbenega inženiringa pojavljajo tudi elementi zastraševanja, šokiranja, izkoriščanja (namišljene) hierarhične nadrejenosti in podobno.

Ravno naivnost v povezavi z nizko ozaveščenostjo uporabnikov je bila temelj prvemu masovnemu primeru izkoriščanja družbenega inženiringa, ki je temeljil na **izkoriščanju zaupanja oz. družbenem inženiringu.**

Izkoriščanje zaupanja

Že dolgo se s pomočjo elektronske pošte širijo virusi, ki se lažno predstavljajo kot sporočilo osebe, ki bi jo prejemnik lahko poznal. Zato se uporabnik pogosto ni mogel upreti skušnjavi in je priponko poskušal odpreti ter tako nehote izvedel zlonamerno kodo, ki se je skrivala v priponki. Virus se je nato razposlal vsem naslovnikom v imeniku uporabnika, nato pa se je lotil uničevanja vseh slikovnih in glasbenih datotek, ki jih je uspel najti.

Virus je torej izkoriščal dejstvo, da zaupanje predstavlja ranljivost, ki jo lahko s pridom izkoristi. Ta ranljivost je bila celo tako velika, da so strokovnjaki po prvem opaženem primeru v pičlih nekaj urah zaznali prizadete sisteme že v 20 državah po svetu.

Predstavljamo primer izkoriščanja družbenega inženiringa z namenom pridobiti informacije o finančnem stanju določenega podjetja, ki je bilo sicer zaupne narave. Povzetek pogovora:

Mi: *»Pozdravljeni, kličemo iz podjetja XXX. Imamo težavo z neplačilom fakture direktorja podjetja YYY, ki je pri nas naročil in prevzel prenosni računalnik, računa pa ni poravnal. Ob prevzemu nam je sicer podpisal jamstvo v obliki menice, za katero pa vemo, da jo je smiselno izkoristiti samo, če račun podjetja YYY ni izpraznjen, saj v nasprotnem primeru ne dobimo nič, menica pa zapade.«*

Uslužbenka: *»Gospod, žal je ta informacija zaupne narave.«*

Mi: *»Gospa, prosimo vas, da nam vsaj malo olajšate stisko, v kateri smo se znašli. Vaš sodelavec ZZ ZZ nas je napotil na vas kot osebo, ki bi nam lahko pomagala.«*

Uslužbenka: *»Poglejte, stanja na računu podjetja YYY vam nikakor ne smem posredovati, lahko pa vam le namignem, da se vam v tem trenutku menice ne splača unovčiti.«*

(vir: osebna izkušnja avtorja)

Čeprav tovrstna informacija ni popolna, lahko že namig zadošča za odločitev o unovčenju menice. Uslužbenka banke je zavestno izdala del zaupne informacije ob apeliranju tako na njeno sočutje kot na prijateljsko vez s sodelavcem.

Mimogrede — kasneje se je izkazalo, da je »podjetnik« podobno, torej z vzpostavljenim zaupanjem s pomočjo menice, opeharil še vrsto podjetij v Sloveniji, zato zdaj sedi za zapahi.

Neodgovorno in nepazljivo ravnanje

Pomanjkanje ozaveščenosti smo navedli med vzvodi za zlorabo informacij že v začetku poglavja. Ljudje se pogosto zavemo pomena zaupne informacije šele takrat, ko je že zašla v javnost, ali pa podatka, ko je že izgubljen. Kljub temu nas incident pogosto ne izuči, saj nam v obilici dela preprosto zmanjkuje časa za organizacijo in varovanje podatkov.

Primer ravnanja, ki povečuje tveganje, je omenjen že v uvodu — geslo je pogosto lažje dobiti z opazovanjem uporabnika pri delu kot pa s pomočjo tehnoloških rešitev. Prav tako preprosto se je usesti za nezaseden računalnik, na katerem se odvija ohranjevalnik zaslona (angl. screen-saver), in poskusiti, ali slučajno ni zaščiten z geslom.

Še pogostejši primer nepazljivega ravnanja je puščanje pomembnih ali zaupnih dokumentov na delovni mizi, vsem na očeh. Vsak mimoidoči ali čakajoči lahko s še tako hitrim pogledom ujame kak košček podatkov, ki mu ni namenjen.

Že samo zavedanje, da posojanje mobilnega telefona tujcu, da »poišče svojega« ali »pokliče kolega«, ni pametno, nas lahko obvaruje nepridiprava, ki bi tako prestregel našo številko.

Nezanemarljiv vpliv na informacijsko varnost predstavlja tudi (ne)odgovorno ravnanje z odsluženimi podatki oz. podatkovnimi nosilci. V Združenih državah se je brskanje po smeteh razpaslo do te mere, da so zanj skovali celo poseben izraz — »dumpster diving«.

Vpliv preusmerjanja pozornosti in prepričljivosti

Čarovnikovi in iluzionistovi triki pogosto temeljijo na preusmerjanju pozornosti, pogosto pa se to dogaja tudi pri zlorabi informacij.

Poglejmo si primer nenapovedanega obiska »serviserja« v podjetju, kjer smo izvajali preizkus ozaveščenosti. Serviser se je pri vhodnih vratih podjetja pojavil, ravno ko je skupina zaposlenih odhajala na malico. Z nasmehom jih je pozval, če mu lahko prosim pridržijo (z dostopno kartico zaščitena) vrata, da mu ne bo treba klicati tajnice, ker je verjetno tudi ona že na malici. Seveda so ga prav tako z nasmeškom spustili v prostore podjetja. Ko je naletel na prvega zaposlenega, ga je brez obotavljanja vprašal, kje se nahaja glavni strežnik, ker »nekaj ne deluje in je treba zadeve preveriti«. Napotke je dobil brez težav. Ko je prišel do pisarne s strežnikom, je vstopil, se predstavil tajnici z lažnim imenom kot predstavnik podjetja XXX (ki temu podjetju sicer vzdržuje računalniško opremo), omenil, da nadomešča običajnega serviserja, in takoj dodal, da ima zelo omejen čas, ker bodo sicer cel dan brez elektronske pošte, zato naj mu čim prej omogočijo dostop do strežniškega računalnika. Ker tajnica na nenadni dogodek ni bila pripravljena, grožnja o »celem dnevu brez e-pošte« pa je bila po njeni oceni dovolj neprijetna, a tudi čisto verjetna, je serviserja brez težav spustila do glavnega strežnika.

Vir opisanega scenarija je prav tako lastna izkušnja avtorja iz nabora preteklih izkušenj. Izveden je bil ob dovoljenju vodstva v javnem podjetju, ki se ukvarja s pripravo in izvedbo razpisov za sredstva EU. Direktor podjetja je bil ob tem prepričan, da jim informacij praktično ni mogoče ukrasti, ker imajo vpeljane odlične tehnične rešitve. Žal pa do trenutka, ko je prejel rezultat preizkusa, ni pripisoval večje teže človeškemu dejavniku. Brez težav si lahko predstavljamo, kaj vse bi se lahko zgodilo, če bi specialista za varnost nadomestila oseba z manj čednimi nameni. Če bi le eden od zaposlenih, s katerimi je prišel serviser v stik, posumil, da nima opravka z dejanskim predstavnikom servisnega podjetja, bi bil končni učinek lahko popolnoma drugačen.

Prepričljivost lahko dosežemo na več načinov — z lažno identiteto oz. impersonacijo, z zlitjem oz. integracijo v ciljno skupino, z razpršitvijo odgovornosti, z avtoriteto ali čisto običajno prijaznostjo.

Kraja informacij

Kraja informacij strogo gledano sicer ni predmet družbenega inženiringa, vendar je z njim v številnih primerih tesno povezana. Kot smo že omenili, lahko s samozavestnim nastopom vstopimo na področja, kjer imamo dostop do zaupnih podatkov. Ponovno sledi primer iz nabora osebnih izkušenj avtorja.

Direktor nekega podjetja se je dlje ukvarjal s problemom, pri katerem je sumil, da gre za krajo informacij. Na slednje je pomislil, ko je pri nekaj zaporednih razpisih izgubil posel, pri tem pa ga je premagal isti konkurent, običajno z le neznatno nižjimi cenami izdelkov. Ker so tako majhne razlike v ceni skoraj nemogoče v panogi, kjer so marže običajno nekaj stoodstotne, je zaključil, da se konkurent na razpise prijavlja z dobrim poznavanjem razpisnih cen direktorjevega podjetja.

Pregled informacijskega sistema ni razkril varnostnih pomanjkljivosti, zato je bila pozornost preusmerjena na zaposlene v podjetju. Direktorjev sum je bil upravičen, saj se je po pregledu dnevnika dostopov izkazalo, da je do sistema še vedno imel dostop bivši komercialist, ki v podjetju že nekaj mesecev ni bil več zaposlen. To je bilo omogočeno izključno zaradi potreb po posredovanju elektronske pošte, saj je bil komercialist v stiku s precej strankami, zato je občasno še vedno prejemal pošto na ta naslov. Ker je komercialistu direktor po odpovedi še vedno zaupal, mu je na njegovo prošnjo odobril dostop, ni pa mogel vedeti, da bo prihodnji delodajalec to izkoristil, saj je po razgovoru za delo vedel, da je komercialist prej delal za konkurenčno podjetje. Ko si je v novem podjetju nastavil povezavo v sistem starega podjetja, je novi delodajalec to lahko preprosto izkoristil, saj je bilo geslo za dostop shranjeno v nastavitvah. Pravice komercialistovega uporabniškega imena se z njegovim odhodom niso spremenile, zato je lahko novi delodajalec dostopal ne le do elektronske pošte, temveč tudi do datotek na strežniku.

Ta primer nas pripelje do še enega načina »kraje« informacij — s pomočjo prevzema zaposlene osebe. V tujini so protikonkurenčne klavzule že pogosta praksa, vendar pa se vseeno najdejo podjetja, ki ponudijo zaposlenemu pri konkurenčnem podjetju višje plačilo, da bi ga privabili k sebi in s tem poskušali pridobiti tudi zaupne informacije, ki jih je zaposleni prej uporabljal.

Najpogostejša oblika kraje informacij še vedno ostaja kraja računalniške opreme skupaj s podatki, ki jih ta vsebuje. Zaskrbljujoče pa je, da so najpogostejše »žrtve« kraj podatkov državni uslužbenci — v ZDA je od januarja 2003 do oktobra 2006 zabeleženih 788 primerov, ki so vključevali kraje ali izgube osebnih ali zaupnih podatkov, med letoma 2001 in 2006 pa so »izgubili« 1137 prenosnih računalnikov.

Ukrepanje ob zaznani zlorabi

Pravilen odziv ob zaznani zlorabi je prav tako pomemben element informacijske varnosti. Prepogosto se namreč dogaja, da poskuša odgovorni za informacije oz. informacijska sredstva (pogosto je to sistemski administrator) primer prikriti in s tem obvarovati svoj ugled ali celo delovno mesto. To pa žal lahko pripelje do še hujših posledic za lastnika informacij. Predstavljajmo si primer, ko skrbnik sistema zazna dostop do baze strank spletne prodajalne neznanega storilca. Sistem poskuša po svojih močeh zavarovati, nato pa prikriti sledove vdora. S tem dejanjem onemogoči dostop pravnemu lastniku informacij (v tem primeru je to podjetje, ki ima prodajalno v lasti) in ovira pravočasno pravilno ukrepanje, prav tako pa pomanjkanje sledi lahko močno oteži iskanje storilca.

Takojšen odziv s posredovanjem suma oz. podrobnosti o incidentu vsem odgovornim je torej priporočljiva politika ravnanja v vseh primerih zlorab. Le tako je namreč mogoče zagotoviti pravilen pristop k zaščiti zlorabljene informacije oz. sistema, določitvi obrambnih mehanizmov, preprečevanju ponovitve incidenta, in ne nazadnje obveščanju javnosti (če je to potrebno).

V primeru hujših incidentov je smiselna prijava ustreznim javnim organom, ki so za to pristojni. Imajo namreč veliko izkušenj z različnimi primeri, prav tako pa sredstva in pooblastila za učinkovito iskanje podrobnosti o incidentu in tudi krivcev. Tako ima lahko javno priznanje mnogo blažje posledice oz. potencialno škodo ugledu, kot pa če se v javnosti izve, da se je poskušalo zlorabo prikriti.

2.7 Vloga ozaveščanja in izobraževanja

Pokazali smo že, da je ozaveščenost tesno povezana s prepričanji zaposlenih glede varovanja informacij.

Hipoteze, navedene v raziskavi [8], potrjujejo povezanost prepričanj zaposlenih o varovanju informacij s ključnimi merili, ki na ta prepričanja vplivajo: prednosti skladnosti, stroški (cena) skladnosti in stroški (cena, posledice) neskladnosti s politiko varovanja informacij.

Eden od najučinkovitejših načinov vpliva na ozaveščenost je izvedba programov ozaveščanja, ki vključujejo prikaz naštetih meril. Cilj programa je običajno izvedba izobraževanj oz. delavnic, katerih namen je okrepiti prepričanja zaposlenih o prednostih, ranljivostih in posledicah skladnega in neskladnega ravnanja.

Seznanitev zaposlenih, torej demonstracija teh meril, oz. udeležba v programu ozaveščanja lahko neposredno in posredno spreminja oz. vpliva na prepričanja zaposlenih o skladnosti z varnostnimi politikami in problematike varovanja informacij na splošno.

Učinkovit program ozaveščanja prav tako zmanjšuje vtis, da skladnost z varnostnimi politikami ovira delovne procese zaposlenih.

Tako organizacija vzpostavlja kulturo varovanja informacij pri vseh zaposlenih in s tem vpliva na ključni — človeški dejavnik.

2.8 Kultura varovanja informacij v organizaciji

Ravnokar navedena poglavja so pregledno povzeta v »Smernicah za varovanje informacijskih sistemov in omrežij«, ki jih je OECD (Organization for economic co-operation and development) pripravila že leta 2002 [19].

Podrobnosti posameznih poglavij ni treba navajati, saj je dovolj že devet komplementarnih načel, ki vključujejo zaposlene (uporabnike) na vseh ravneh (vodstvenih in operativnih):

a) ozaveščenost: uporabniki naj se zavedajo potrebe po varovanju informacijskih sistemov in omrežij ter kaj lahko storijo za povečanje varnosti;
b) odgovornost: vsi uporabniki so odgovorni za varnost informacijskih sistemov in omrežij;
c) dovzetnost: uporabniki naj pravočasno in kooperativno preprečujejo, zaznavajo in ukrepajo v primeru varnostnih incidentov;
d) etika: uporabniki naj spoštujejo legitimne interese drugih;
e) demokracija: varnost informacijskih sistemov in omrežij naj bo v skladu s ključnimi vrednotami demokratične družbe;
f) ocena tveganj: uporabniki naj izvedejo oceno tveganj, da se ugotovijo grožnje in ranljivosti, ter določijo sprejemljivo raven tveganj;
g) varnostni načrt in implementacija: uporabniki naj vključujejo varnost kot ključen element informacijskih sistemov in omrežij tako v smislu tehničnih kot netehničnih ukrepov in rešitev;
h) upravljanje z varnostjo: uporabniki naj sprejmejo celovit pristop zagotavljanja varnosti, vključno z varnostnimi politikami, praksami, ukrepi in postopki;
i) ponovna ocena: udeleženci pregledajo in ocenijo varnost informacijskih sistemov in omrežij ter poskrbijo za ustrezne spremembe varnostne politike, praks, ukrepov in postopkov.

Pomembnost navedenih načel so pokazale citirane študije in raziskave. Določene izmed njih želimo izpostaviti tudi v tem delu in s pomočjo zastavljenih izhodiščnih trditev potrditi ustreznost oz. pomembnost teh načel. V nadaljevanju bomo s pomočjo treh pristopov k analizi človeškega dejavnika podrobneje obravnavali načela ozaveščenosti, odgovornosti in dovzetnosti ter ocene tveganj.

3 Analiza človeškega dejavnika

Pomembnost človeškega dejavnika glede varovanja informacij s(m)o že pokazali. S pomočjo raziskave želimo pokazati, v kolikšni meri je varovanje informacij odvisno od človeškega dejavnika. V ta namen smo najprej oblikovali raziskovalna vprašanja, ki izhajajo iz teoretičnih spoznanj in postavljajo okvir raziskovanja deleža človeškega dejavnika v varovanju informacij.

Za raziskavo človeškega dejavnika smo postavili tri raziskovalna vprašanja:

R1: Kolikšen je delež človeškega dejavnika pri varovanju informacij?

R2: Ali so uporabniki v slovenskih organizacijah dovolj ozaveščeni glede varovanja informacij?

R3: Kako lahko učinkovito izboljšamo ozaveščenost zaposlenih v organizaciji?

Na podlagi raziskovalnih vprašanj smo oblikovali izhodiščne trditve, ki jih bomo poskušali potrditi z uporabo treh različnih analitičnih pristopov:

1. **kvantitativna analiza tveganja z uporabo lastnega orodja za analizo;**
2. **uporaba družbenega inženiringa in intervjujev za prikaz stopnje ozaveščenosti;**
3. **merjenje učinkov delavnic ozaveščanja v referenčni organizaciji s pomočjo vprašalnikov pred in po delavnici.**

Izhodiščne trditve, ki smo jih oblikovali, so:

T1: Človeški dejavnik je odgovoren za več kot polovico incidentov, povezanih z varovanjem informacij v organizaciji.

T2: Zaposleni v slovenskih organizacijah so premalo ozaveščeni glede varovanja informacij.

T3: Za doseganje višje stopnje varovanja informacij v organizaciji je ozaveščanje zaposlenih ključnega pomena.

V uvodnem poglavju analize bomo izvedli oceno tveganja informacijske varnosti na primeru svetovalnega podjetja, katere cilj je opredeliti delež, ki ga v skupnem tveganju predstavlja človeški dejavnik. Uporabljena metodologija analize tveganja je kvantitativne narave in izhaja iz priporočil standardov [1, 3] ter uporablja nabore groženj in ranljivosti, kot jih navajajo dobre prakse. Kot dodatni element bo analiza tveganja upoštevala tudi finančni

vidik tveganj, ki je za vodstvo organizacij ključnega pomena, saj omogoča učinkovitejše razporejanje virov, namenjenih varovanju informacij [7].

Izveden poskus družbenega inženiringa ima za cilj ugotoviti, ali so zaposleni v organizacijah primerno ozaveščeni glede zaznavanja in pravilnega ukrepanja ob prejemu vsebine neznanega izvora. Intervjuji z vsemi vključenimi organizacijami imajo namen pridobiti dodatne informacije o njihovih postopkih in pristopu k varovanju informacij.

Menimo, da je bila priložnost, da imamo v pričujoči raziskavi možnost prikazati tudi učinek delavnice ozaveščanja v konkretni organizaciji v slovenskem okolju, ugodna. S pomočjo anket pred in po delavnici bomo poskušali ugotoviti, kako ozaveščanje zaposlenih vpliva na njihov odnos do varovanja informacij in kakšen pozitiven učinek lahko prinese.

Potek raziskovalnega dela je skiciran na diagramu 9.

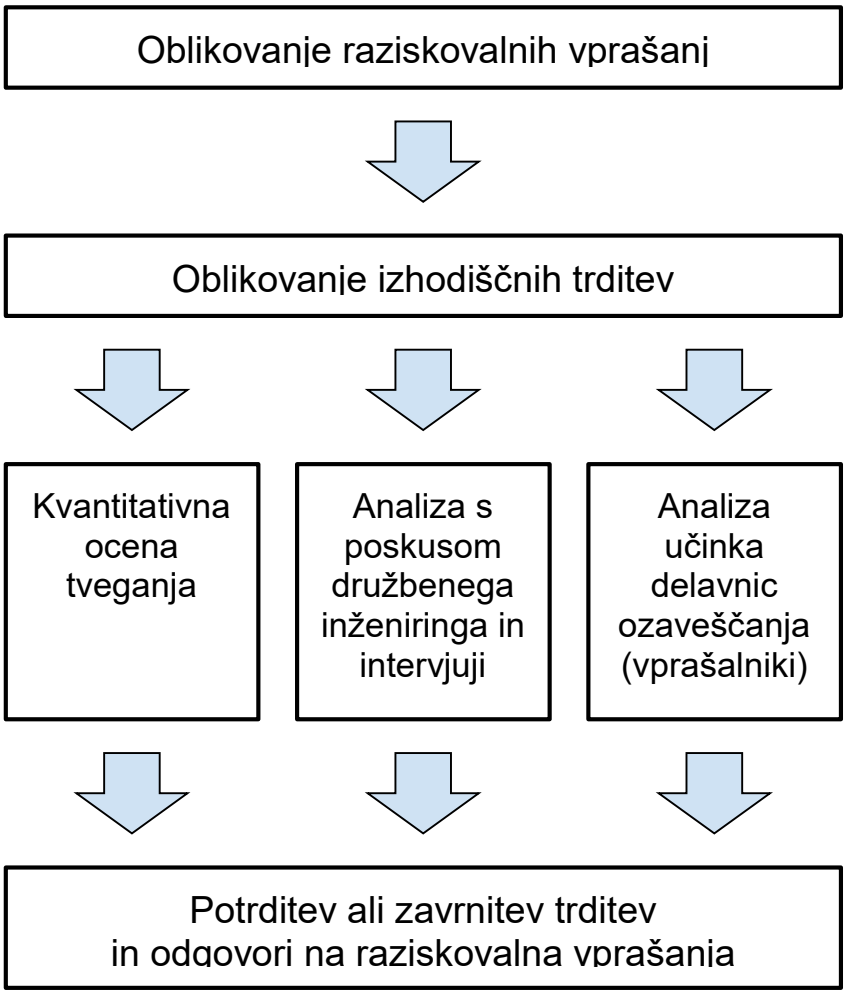


Diagram 9: Potek raziskovalnega dela

3.1 Kvantitativna ocena tveganja

3.1.1 Teoretična podlaga analize

Pri pregledu dobrih praks smo pokazali, da večina standardov priporoča ali zahteva izvedbo ocene tveganja. Ta kontinuiran ali periodičen proces je namenjen identifikaciji in vrednotenju groženj in ranljivosti, povezanih z varovanjem informacijskih tokov in informacij (v vseh oblikah), kot nastopajo v organizaciji.

3.1.2 Orodje SBR

Avtor magistrske naloge je razvijal ali vodil razvoj orodij za oceno tveganj varovanja informacij že od leta 2005, ko je začel nadgradnjo certifikatov za implementacijo in vodilnega presojevalca po standardu BS 7799:1999 na osveženo različico ISO/IEC 27001:2005.

Sprva preprosto enouporabniško orodje, razvito v programskem jeziku Delphi, se je na podlagi povpraševanja na trgu razvilo v napredno večuporabniško spletno aplikacijo, najprej pod imenom RAA (Risk Assessment Accelerator), nato pa kot Silver Bullet Risk (SBR), katerega razvoj je avtor vodil med letoma 2010 (prva komercialna različica) in 2014.

V tem času je orodje vpeljano v številna večja organizacijska okolja v Sloveniji: Abanka, ATVP, Dravske elektrarne, ELES, Mikrografija, MORS idr.

Čeprav noben izmed standardov ne določa natančne metodologije, po kateri mora organizacija izvajati oceno tveganja, pa vseeno številni standardi in dobre prakse navajajo ključne elemente, ki jih mora ocena tveganja zajemati, ter končne cilje, ki jih mora zasledovati. Vsem tem elementom in ciljem je sledil tudi omenjeni razvoj orodja SBR, ki zato omogoča izvedbo ocene tveganja skladno s standardi ISO/IEC 27001, ISO 22301 in drugimi. Poleg skladnosti omogoča še vrsto prednosti, kot so sočasno delo več uporabnikov, centralizirani nabori groženj in ranljivosti, testiranje scenarijev in zgodovinska primerjava, večjezičnost, prilagodljivost metodologij, poročil in podobno.

Ena od prednosti končne različice okolja je neposredno vključevanje vodstvene strukture v proces ocene tveganja. Vodje procesov tako določijo vpliv posameznih sistemov (hierarhije virov, sredstev) na njihov proces, ni pa se jim treba ukvarjati z verjetnostmi pojava posameznih groženj ali ranljivosti. Te nato določijo drugi odgovorni, npr. vodje informacijske varnosti, neprekinjenega poslovanja.

Na podlagi vpliva na poslovanje in vrednotenja groženj se nato samodejno ustvari register tveganj. Ker je uporabljena metodologija kvantitativna, so stopnje verjetnosti in vpliva

(škode) v matriki opremljene z določenimi okvirnimi vrednostmi, zato je mogoče tveganja izraziti tudi finančno. Tak register vodstvu predstavlja odlično podlago za ukrepanje, saj lahko namensko ravna z viri za odpravo tveganj, ki predstavljajo največji vpliv na poslovanje organizacije.

3.1.3 Primer organizacije

Zaradi zaupnosti podatkov ne moremo navajati podatkov dejanskih analiz organizacij, ki so uporabljale orodje SBR. Lahko pa izvedemo poskus ugotavljanja deleža človeškega dejavnika pri analizi, ki je pripravljena za vzorčno organizacijo — v tem primeru svetovalno-razvojnega podjetja, ki odraža sliko dejanskega podjetja, kjer je bil zaposlen avtor.

Uporabili bomo enak nabor groženj in ranljivosti, kot je bil pripravljen za vzorčno organizacijo, med njimi pa identificirali tiste, ki so neposredno odvisne od človeškega dejavnika, nato pa prikazali razliko med končnimi tveganji za organizacijo, če človeški dejavnik iz ocene tveganja odstranimo.

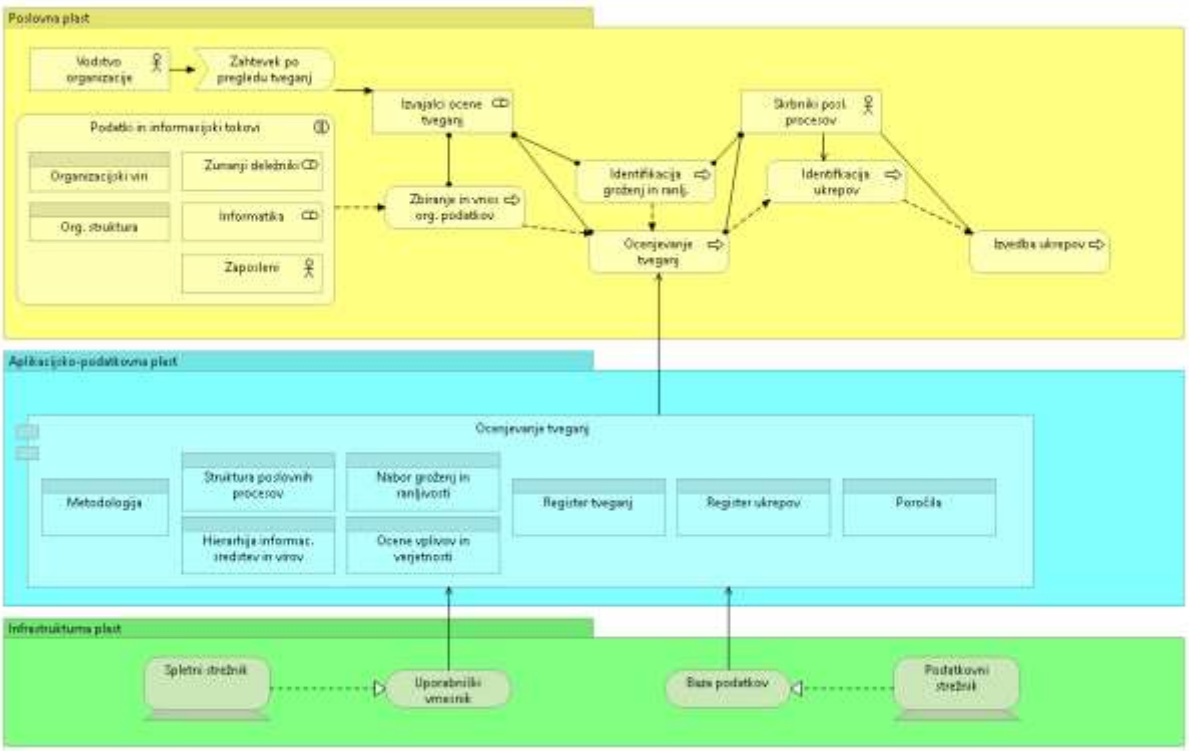
Podrobnosti izvedbe analize in dela z orodjem presegajo obseg naloge, predstavili pa bomo vse ključne elemente in postopke metodologije ter tako definirali podlago za izvedbo ocene teže človeškega dejavnika.

3.1.4 Delo v orodju SBR

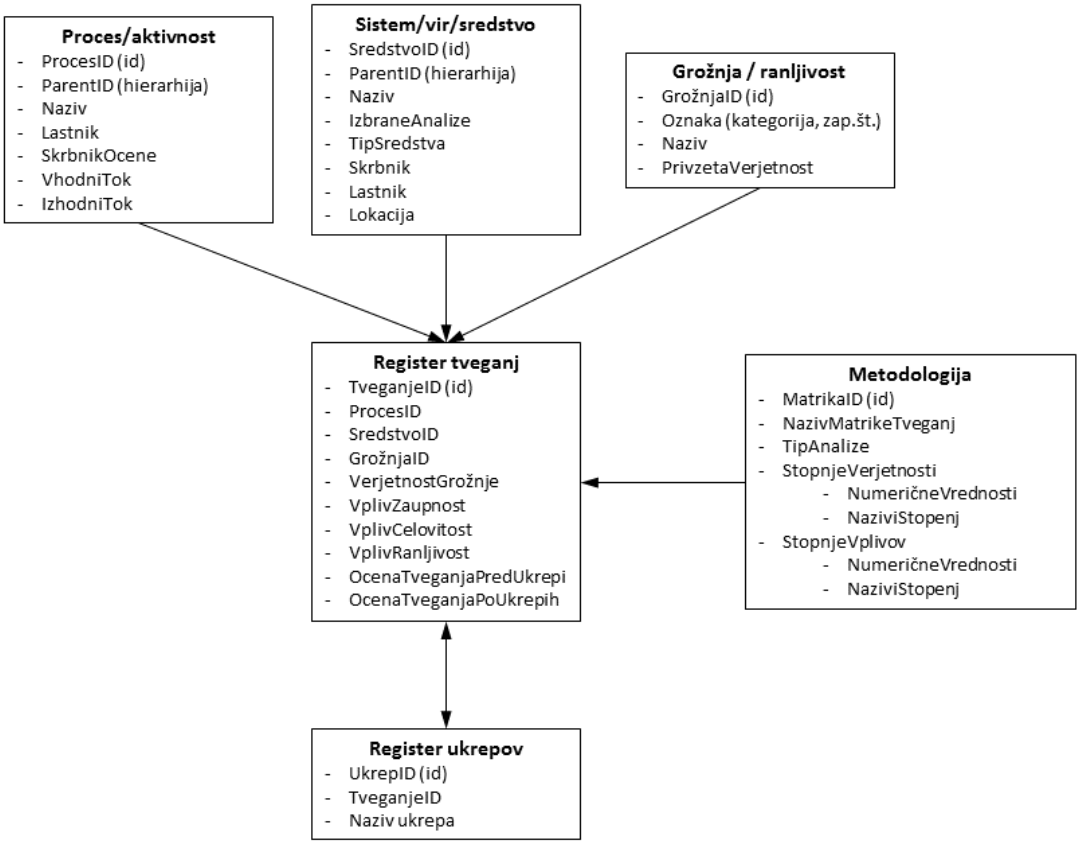
Ponazoritev poteka dela v orodju SBR, vključenih akterjev, ključnih dejavnosti, podatkovnih elementov in osnovnih povezav je s pomočjo UML-diagrama prikazana na sliki 10. Diagram je pripravljen v odprtokodnem orodju Archi in loči elemente na tri plasti: poslovno, aplikacijsko in infrastrukturno.

Za boljšo predstavo podatkovnega modela je slika 11, ki prikazuje povezavo treh ključnih elementov, ki so potrebni za izgradnjo registra tveganj: Proces, Sredstvo in Grožnja ter Metodologija, ki določa način vrednotenja posameznega tveganja. Posamezno tveganje ima lahko dve oceni:

- preden so zanj vpeljani ukrepi,
- po vpeljanih ukrepih.



Slika 10: UML-diagram orodja SBR



Slika 11: Razredni diagram orodja SBR

3.1.5 Izvedba ocene v orodju SBR

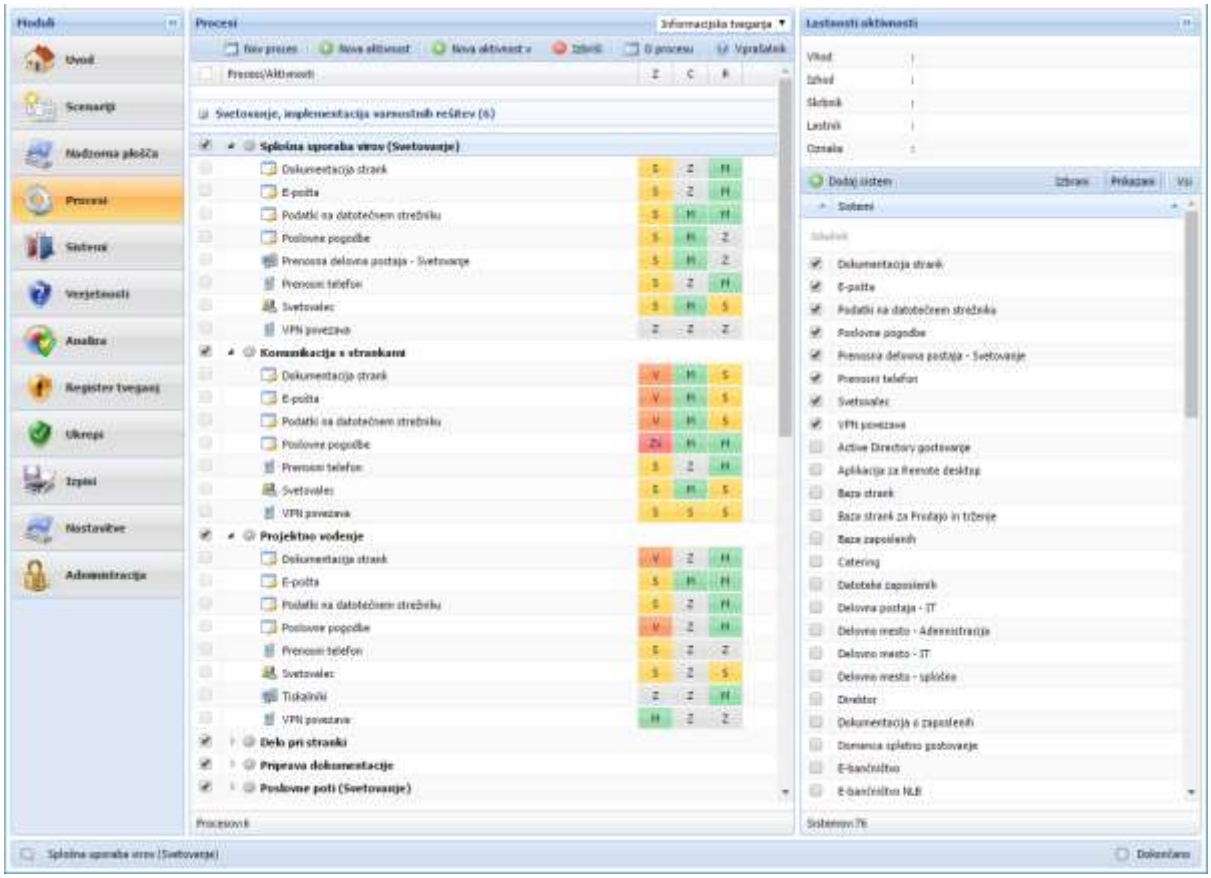
Po prijavi se uporabniku prikažejo nabor modulov (levo) [slika 12], vsebina izbranega modula (sredina) in nastavitve oz. parametri modula (desno). Vsak modul omogoča izvedbo posameznega koraka v oceni tveganja.

Slika 12: Uvodni zaslon orodja SBR

Na desni strani uvodnega zaslona je preprost kontrolni seznam, s pomočjo katerega označimo, katera opravila, potrebna za izvedbo ocene, smo že izvedli, katera pa še čakajo na izvedbo.

3.1.5.1 Definiranje procesov organizacije

Vzorčno podjetje izvaja vrsto procesov, ki so sestavljeni iz posameznih aktivnosti, te pa potrebujejo za svojo izvedbo določene sisteme [slika 13].

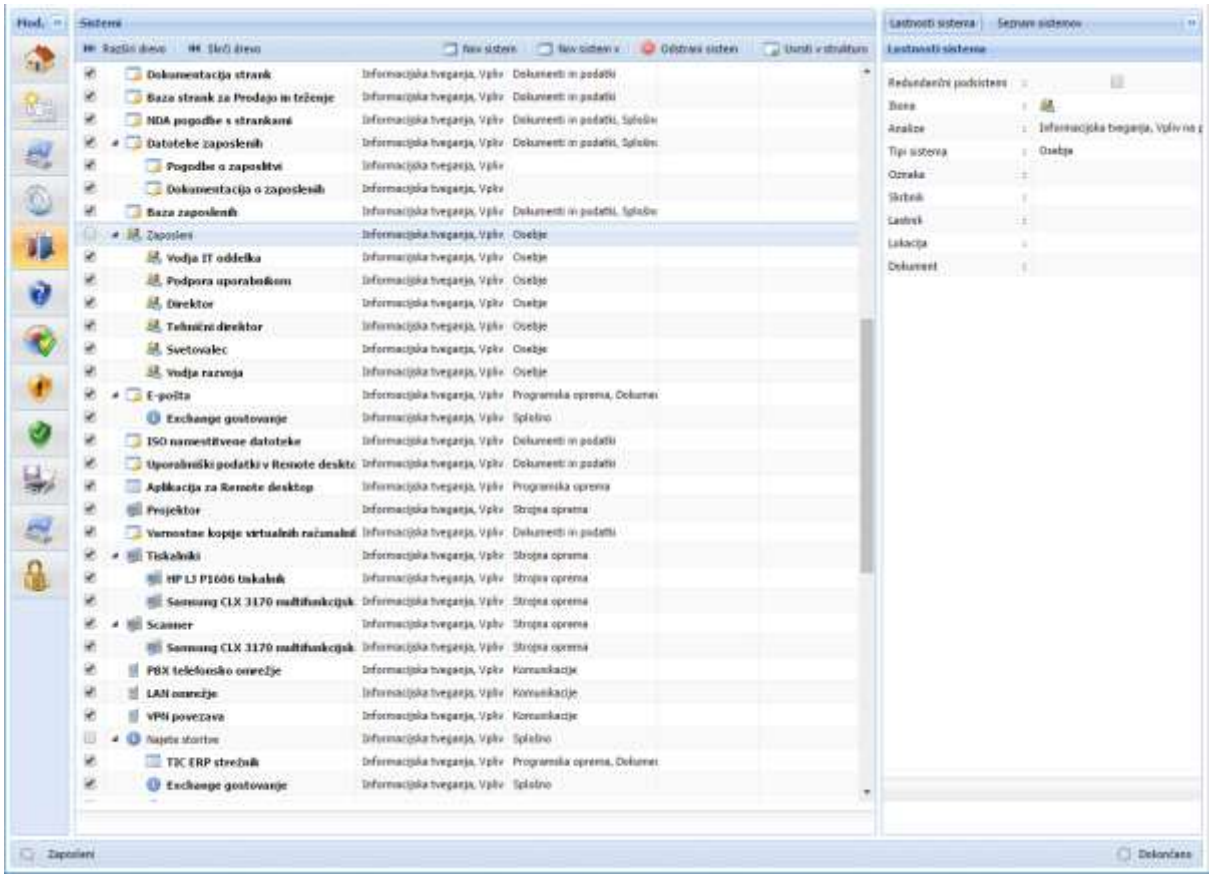


Slika 13: Procesi z oceno vpliva in vključenimi sistemi

Za vsak sistem pri posamezni aktivnosti ocenimo vpliv na poslovanje tako, da opredelimo škodo, ki lahko nastane za zaupnost, celovitost ali razpoložljivost sistema oz. povezane aktivnosti. Škodo oz. vpliv ocenjujemo z diskretnimi vrednostmi, ki so vnaprej določene v matriki tveganja.

3.1.5.2 Definiranje virov in sredstev organizacije

Pod pojmom sistemi so opredeljeni vsi viri in sredstva, ki jih organizacija potrebuje za svoje delovanje: prostori, informacijska infrastruktura, dokumenti, podatki, zaposleni in drugi. Pojem sistem definira hierarhično strukturo, v katero lahko združujemo posamezne vire — npr. sistem “Poštni strežnik” je lahko sestavljen iz dveh redundantnih virtualnih strežnikov “Strežnik 1” in “Strežnik 2”, ki tečeta na dveh fizično ločenih strežnikih, ki pa se nahajata v različnih poslovnih prostorih organizacije. Organizacija lahko vpelje poljubno kompleksnost sistemov, kar posledično pohitri izvedbo ocene tveganja — npr. verjetnost grožnje “Naravne nesreče — Potres” lahko ocenimo le enkrat za posamezno poslovno stavbo, nato pa se prenese na vse vire, ki se v tej stavbi nahajajo.

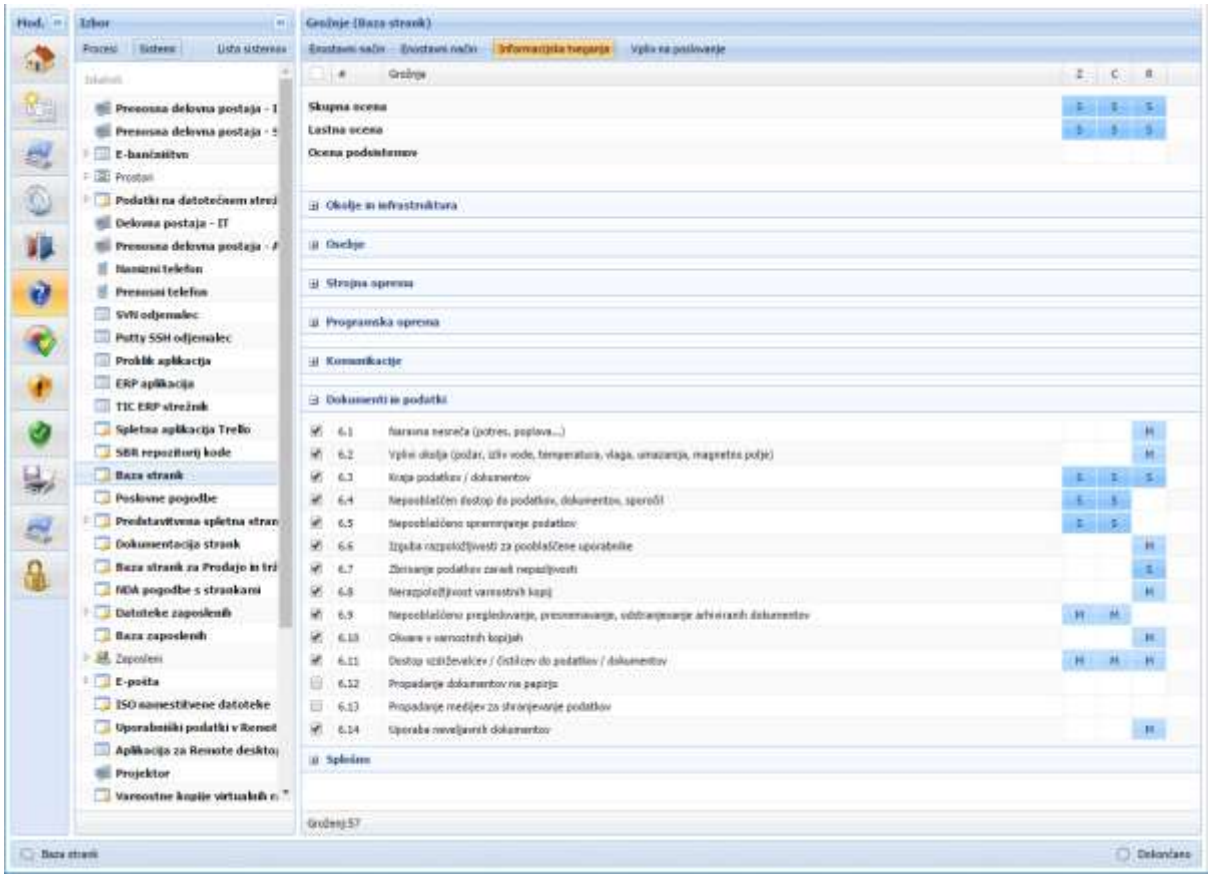


Slika 14: Hierarhija sistemov (virov in sredstev)

Za posamezne sisteme lahko opredelimo, v katero skupino sredstev spadajo (strojna, programska oprema, podatki, osebje, infrastruktura, komunikacije, splošno), katere analize tveganj bomo zanje izvajali in številne druge parametre.

3.1.5.3 Ocena verjetnosti groženj in ranljivosti

Naslednji korak v oceni tveganja je ocena verjetnosti, s katero lahko nastopi posamezna grožnja oz. je lahko izkoriščena posamezna ranljivost. Verjetnost tveganja tako za ogrožanje zaupnosti kot celovitosti in razpoložljivosti ocenjujemo po treh merilih (zaupnost, celovitost, razpoložljivost).

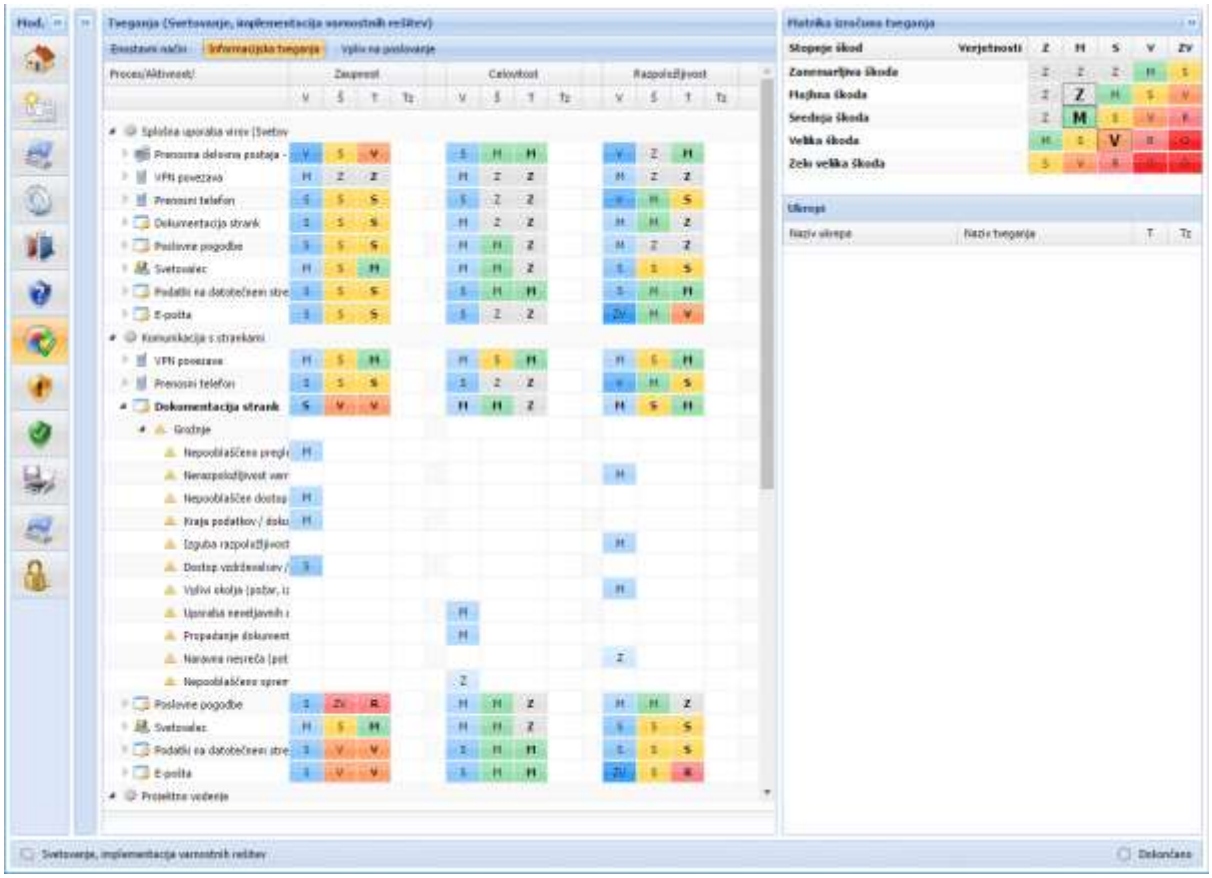


Slika 15: Ocenjevanje verjetnosti groženj in ranljivosti za posamezen sistem

Verjetnost je običajno enaka za vsa tri merila, ni pa nujno, da ima grožnja vpliv na vse tri, lahko le na dva ali enega, kot je razvidno s slike 15.

3.1.5.4 Pregled registra tveganj

Ko smo vnesli verjetnosti groženj in vpliv sistemov na procese v organizaciji, se nam samodejno ustvari register tveganj. Tveganja lahko pregledujemo za posamezen proces, povezan sistem in konkretno grožnjo, zaradi katere tveganje nastopi.

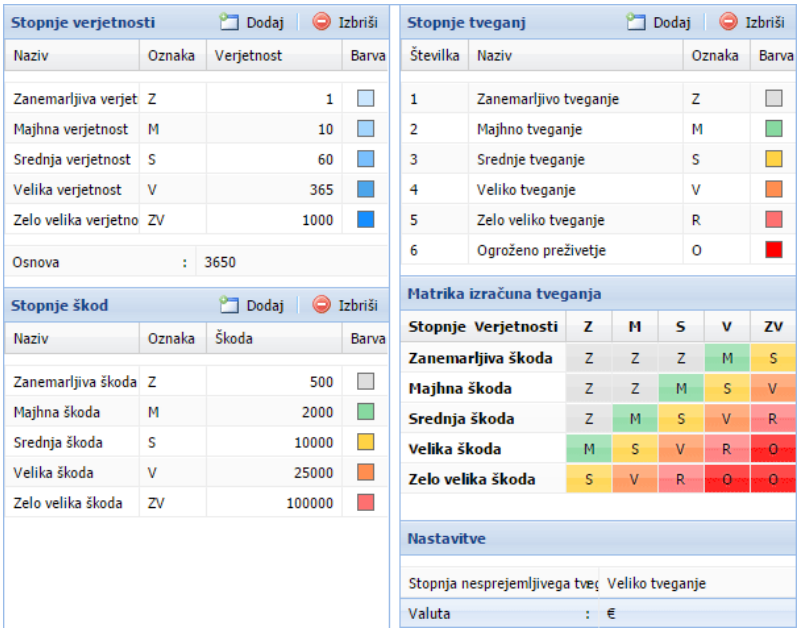


Slika 16: Register tveganj

Iz registra lahko hitro razberemo največja tveganja za organizacijo. Tveganja za izbrani sistem (v tem primeru “Dokumentacija strank”) so označena tudi v matriki tveganj zgoraj desno.

3.1.5.5 Skupni pregled tveganj

Kot smo omenili v začetku poglavja, omogoča orodje tveganja izraziti tudi v finančnem smislu. V vzorčnem primeru smo uporabljali tveganja s šestimi stopnjami, kot so prikazane zgoraj desno na sliki 17. Stopnje tveganj so nato razporejene v 5 x 5 matriko tveganj (spodaj desno).



Slika 17: Matrika tveganj s stopnjami verjetnosti in škode

Pri opredelitvi kategorij verjetnosti smo za osnovo vzeli obdobje 10 let. Stopnje verjetnosti si nato sledijo:

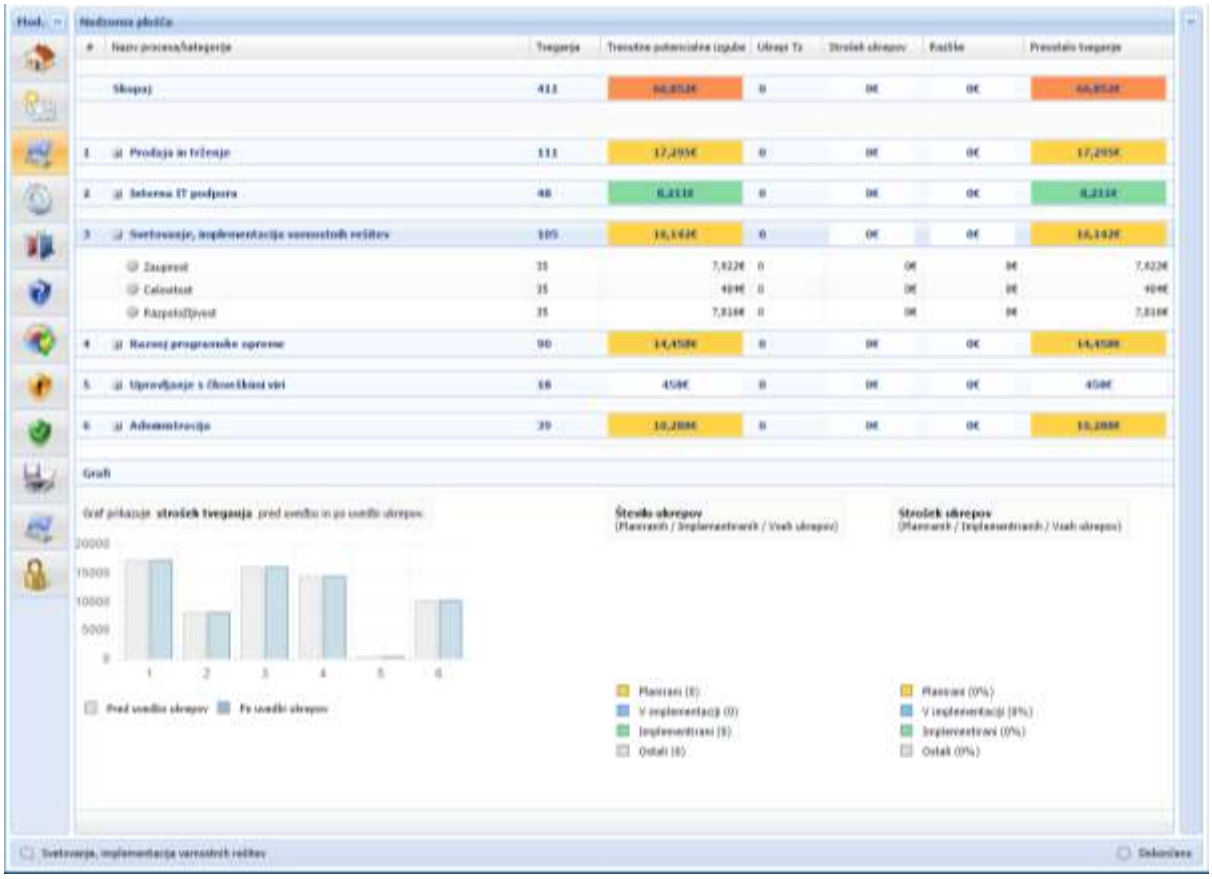
- zanemarljiva verjetnost (~ enkrat na deset let),
- majhna verjetnost (~ enkrat letno),
- srednja verjetnost (~ enkrat na dva meseca),
- velika verjetnost (~ enkrat mesečno),
- zelo velika verjetnost (~ dvakrat tedensko).

Stopnje vpliva oz. škode izrazimo finančno v enoti EUR v razredih:

- zanemarljiva škoda (500 €),
- majhna škoda (2.000 €),
- srednja škoda (10.000 €),
- velika škoda (25.000 €),
- zelo velika škoda (100.000 €).

Diskretne vrednosti v matriki so sicer opisne, vendar ima vsaka izmed njih zadaj matematično določeno vrednost tveganja, ki je produkt verjetnosti in škode. Posledično ima tudi vsaka grožnja na sistemu, ki je potreben za izvajanje procesa, finančno izraženo tveganje. Ko vsa tveganja med seboj seštejemo, pridemo do številke, ki predstavlja potencialno škodo, ki jo lahko organizacija utrpi v določenem obdobju, v našem primeru 10 let.

Škoda za posamezen proces in celotno organizacijo je prikazana v nadzorni plošči, ki jo aplikacija namenja vodstvu kot osnovno orodje za nadzor nad tveganji in je prikazana na sliki 18.



Slika 18: Nadzorna plošča informacijskih tveganj

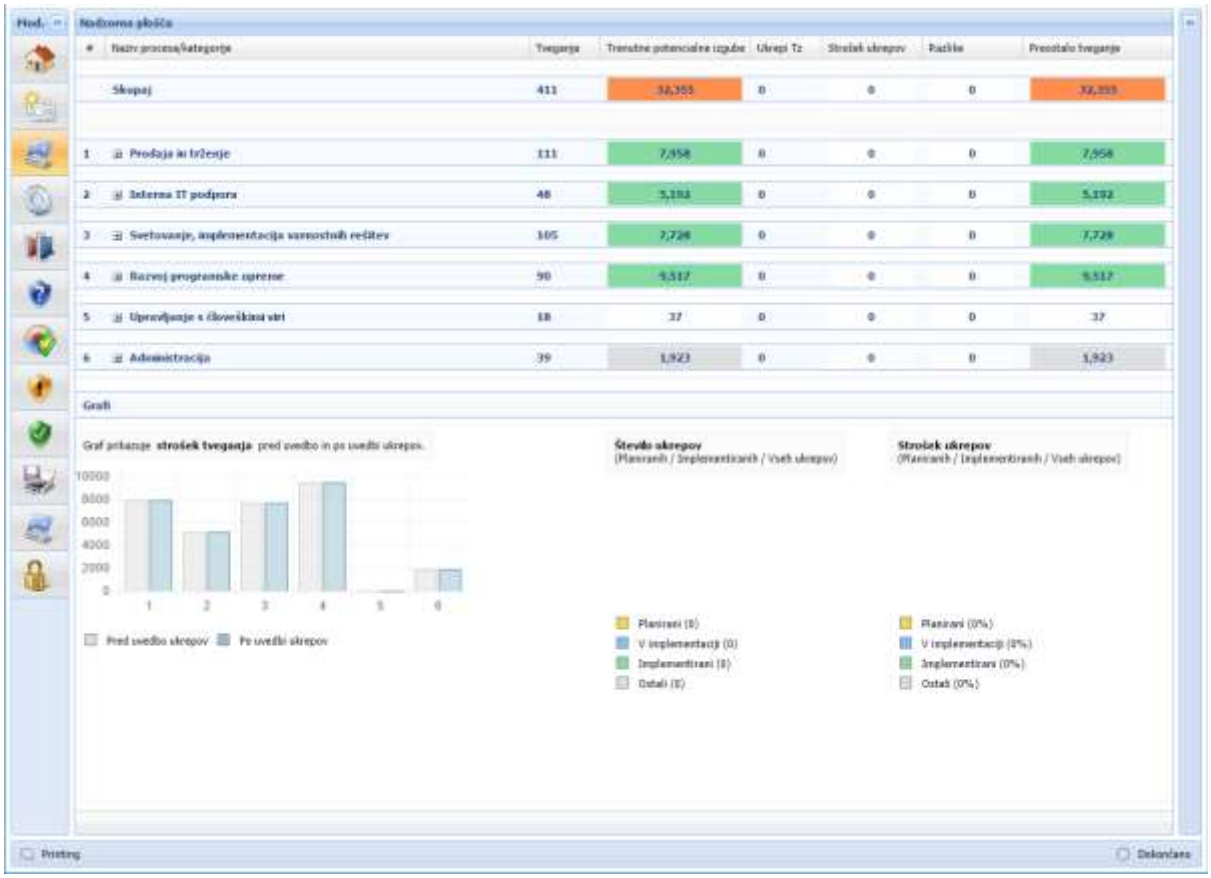
Za posamezen proces so prikazana tveganja za osnovne tri kategorije (zaupnost, celovitost, razpoložljivost), grafi pa prikazujejo stopnjo pred (morebitnimi) vpeljanimi ukrepi in po njih.

S slike lahko razberemo, da znaša skupna višina tveganja za našo vzorčno organizacijo približno 67.000 EUR v obdobju 10 let. Ta številka je seveda okvirna, vendar predstavlja dovolj dobro izhodišče za določanje višine sredstev, ki jih bomo namenili posameznim ukrepom.

3.1.5.6 Delež groženj človeškega dejavnika v vzorčni oceni tveganja

Če želimo oceniti, kolikšen je delež groženj, ki jih v skupnem tveganju predstavlja človeški dejavnik, je dovolj, da iz nabora groženj odstranimo vse tiste, ki so neposredno odvisne od človeškega dejavnika. Iz našega nabora [priloga 5], ki ga je sicer dolga leta uporabljalo oz.

priporočalo tudi Združenje bank Slovenije, smo odstranili vsa tveganja, obarvana zeleno. Končni rezultat v nadzorni plošči je prikazan na sliki 19.



Slika 19: Pregled tveganja z izločenim človeškim dejavnikom

Skupna višina tveganj v istem obdobju se je ob izločenih grožnjah človeškega dejavnika spustila za več kot polovico na dobrih 32.000 EUR.

Na praktičnem primeru smo tako pokazali, da je lahko teža človeškega dejavnika tudi več kot 50 % glede na skupno višino vseh tveganj v organizaciji. Če bi upoštevali, da lahko človeški dejavnik pomaga preprečevati ali omiliti posledice tudi pri tehničnih in naravnih grožnjah, je lahko ta odstotek še višji.

Z uporabo kvantitativnega pristopa k oceni tveganja smo tako na našem primeru potrdili izhodiščno trditev T1.

Vprašanje R1 je v veliki meri odvisno od tipa organizacije, v kateri panogi deluje oz. posluje, in izpostavljenosti določenim grožnjam. Vsekakor pa opisani primer in tudi številne druge raziskave [22, 23] potrjujejo, da delež človeškega dejavnika najpogosteje predstavlja

večinsko težo v skupnem pogledu varovanja informacij in da je lahko v veliki meri kriv za končno škodo, ki v primeru incidenta nastane [9].

3.2 Raziskava s pomočjo družbenega inženiringa

V poglavju 2.6 smo izpostavili pomen družbenega inženiringa oz. zlorabe zaupanja pri varovanju informacij. Za pridobivanje konkretnih rezultatov iz našega okolja smo za potrebe raziskave izbrali družbeni inženiring kot način, ki lahko osvetli ozaveščenost zaposlenih v organizacijah in njihovo pripravljenost na grožnje, ki prihajajo iz okolice in so neposredno odvisne od človeškega dejavnika v organizaciji.

Pristop je imel poleg pridobitve povratnih informacij tudi to prednost, da nam je v večini primerov pomagal odpreti vrata do odgovornih za informacijsko varnost v organizaciji. Vse organizacije smo po zbranih rezultatih poklicali in s pomočjo dodatnih vprašanj oz. intervjuja poskušali izvedeti, kakšen je njihov pristop k varovanju informacij.

Vprašanja so se glasila:

1. Kaj se je dogajalo s ključkom v vašem podjetju/organizaciji?
2. Kdo je odgovoren za sprejem pošte (delovno mesto)?
3. Kakšna navodila ima?
4. Imate v organizaciji pravila, ki opredeljujejo pravilno ravnanje s ključki USB oz. drugo IT-opremo?
5. Vaše stališče ob prejemu ključka? Vaše stališče zdaj?
6. Ali imate notranji ali zunanji IT?
7. Ali in kako skrbite za ozaveščanje uporabnikov?
8. Ali se strinjate, da so zaposleni pogosto premalo ozaveščeni v tem pogledu?
9. Menite, da bi delavnice ozaveščanja o varovanju informacij koristile zaposlenim?

Vprašanj pogosto nismo mogli postaviti do konca ali pa sploh, saj se je kontaktnim osebam mudilo oz. niso želele odgovarjati.

3.2.1 Izvedba družbenega inženiringa

Med junijem in septembrom 2015 smo v ekipi Safe Mode (sodelovanje podjetja Zupo s Fakulteto za varnostne vede) izvedli raziskavo na temo družbenega inženiringa in njegovega vpliva na varovanje informacij. Rezultati so bili nekoliko presenetljivi, zato smo se odločili, da obseg raziskave razširimo na še večji vzorec zajetih organizacij in rezultate združimo.

V prvotni raziskavi smo naključno izbrali 25 malih in srednje velikih organizacij v osrednjeslovenski regiji. V razširjeno raziskavo smo vključili še 61 naključno izbranih srednje velikih in velikih organizacij. Merila za izbor so bila: vse organizacije so iz osrednjeslovenske regije, število zaposlenih se giblje med 15 in 5000, prihodke v letu 2014 pa so zaključile s pozitivnim poslovnim izidom. S pomočjo zadnjega merila smo omejili vzorec, saj smo se želeli izogniti organizacijam, ki bi jim finančne težave morebiti preprečevale učinkovito vpeljavo varovanja informacij. Prav tako menimo, da od uspešnih organizacij v pogledu varovanja informacij vsi deležniki (partnerji, stranke, lastniki) pričakujejo vsaj toliko, če ne več, kot bi pričakovali od povprečne ali podpovprečne organizacije. Vsekakor pa je pri morebitnem posploševanju treba upoštevati navedene omejitve.

Tokrat smo v raziskavo vključili tudi javni, zdravstveni in bančni sektor. Ključ USB smo poslali po pošti v pisemski ovojnici s priloženim dopisom, da smo ključek našli pred vhodom v naslovnikovo organizacijo in da ga vračamo, saj ta vsebuje pomembne podatke. Na ključku je bilo več datotek in dve mapi. Mapa "Slike" je vsebovala nekaj naključnih fotografij, ki smo jih našli na internetu, druga mapa pa je bila poimenovana z imenom podjetja, ki smo mu pismo poslali, in je vsebovala datoteko "Gesla.html". V osnovni mapi sta se nahajali še datoteki "Mail-dostop.html" in "SluzbeniDokumenti.html".

Ko so uporabniki odprli katero od html datotek na pomnilnem mediju, se jim je v spletnem brskalniku pokazalo obvestilo, da se zahvaljujemo za sodelovanje v raziskavi in da bo vodstvo organizacije kmalu obveščeno o rezultatih. V ozadju smo vzpostavili avtomatizirano analitiko evidentiranja zahtevkov, ki so se sprožili ob odpiranju datoteke, iz katere je bilo razvidno, kdaj je določena organizacija odprla določeno datoteko, katera je bila ta datoteka in identiteta organizacije, saj smo vsaki organizaciji namenili unikaten USB-ključek.

3.2.2 Merjenje odziva in intervjuji z organizacijami

Raziskava je potekala v dveh delih. V prvem delu smo želeli ugotoviti, koliko podjetij bo ključ USB uporabilo, v drugem delu pa smo vsa sodelujoča podjetja poklicali in od njih želeli izvedeti:

- Kaj se je s pošto oz. ključem USB dogajalo v podjetju?
- Ali ima določeno podjetje vpeljane varnostne politike za področje informacijske varnosti ali vsaj pravilnik o ravnanju z določenimi napravami, kot so pomnilni mediji in druge naprave?
- Ali v podjetju izvajajo izobraževanja na področju informacijske varnosti in kako pogosto to počnejo?

3.2.3 Analiza rezultatov

V primerjavi s prvo izvedbo raziskave, kjer smo zajeli 25 slovenskih organizacij, smo tudi v drugi izvedbi raziskave dobili podobne rezultate. Tudi tokrat je od 61 organizacij kar **90 %** le-teh ključ USB uporabilo. S temi podatki lahko dodatno utemeljeno domnevamo, da v prvi raziskavi ni šlo le za naključje in da devetdesetinski delež uporabe ključa USB odraža realno sliko v slovenskem prostoru.

Pri načinu ravnanja s prispelo pošiljko v primerjavi s prvo raziskavo prav tako ni večjih posebnosti. Po prejemu pošte je ključek v 11,1 % prišel v roke IT-službe, potem ko so ga ostali zaposleni že uporabili na računalnikih, priklopljenih na omrežje organizacije. V 13 % je IT-služba prva prišla do USB-ključka in ga uporabila sama, kot so dejali, v zavarovanih pogojih na računalnikih, ki niso bili priklopljeni neposredno na omrežje organizacije.

S pomočjo sledenja odpiranju ključkov smo nadalje ugotovili, da je 7,4 % organizacij zanikalo, da je kakršnakoli pošiljka, ki bi ustrezala našemu opisu, prišla na sedež njihove organizacije, čeprav je jasno, da so ključek uporabili (včasih tudi večkrat). To zanikanje niti ni presenetljivo, saj na splošno organizacije nerade govorijo o kakršnihkoli varnostnih luknjah, še posebej na področju informacijske varnosti, saj bi tovrstno razkritje lahko škodilo njihovemu ugledu. S tega vidika je omenjeni odstotek pravzaprav majhen. 9,5 % organizacij pa ni zanikalo, da bi ključek USB dobilo, so pa dejali, da nimajo zabeleženo, da bi takšna pošiljka prišla do njih. Ob tem so organizacije nehote razkrile, da so prisotne pomanjkljivosti pri beleženju dohodne pošte in njeni nadaljnji distribuciji znotraj organizacije.

Izvajanje izobraževanja zaposlenih v organizaciji na področju varovanja informacij je tudi tokrat pričakovano na nizki stopnji. Le 13 % organizacij izvaja izobraževanja za svoje zaposlene, od tega jih 7,4 % meni, da so zaposleni premalo izobraženi na tem področju. Ugotovili smo, da zaposleni na splošno vedo, da so vsakodnevne grožnje varovanju informacij prisotne, vendar ne razumejo, kako. Zaposleni se zavedajo, da so vdori v njihov informacijski sistem sicer mogoči, vendar ne razumejo, kako bi se to lahko zgodilo in posledično tudi niso zmožni prepoznati grožnje, ki je pred njihovimi očmi. Za primer lahko navedemo kar omenjeno raziskavo s ključem USB. Uporabniki vedo, da obstajajo virusi, trojanski konji in druge metode, ki jih lahko ogrožajo, vendar pozabijo, da se lahko prenašajo tudi preko pomnilnih medijev in zato v ključku neznanega izvora v večini primerov ne prepoznajo nevarnosti, saj so bili uspešno zavedeni s pomočjo družbenega inženiringa v obliki dopisa, kjer je pisalo, da USB-ključek vračamo lastniku.

V 14,8 % zaposleni niso vedeli za nikakršne varnostne politike ali vpeljane standarde, 3,7 % pa jih je dejalo, da ima organizacija, ki je njihov lastnik, svoje varnostne politike. Sicer smo

preko telefonskega pogovora ugotovili, da ima 24,1 % organizacij vpeljane različne varnostne politike ali katerega od standardov (običajno iz serije ISO 9000 ali ISO 14000). Uporabniki so, ko so bile njihove lastne ali varnostne politike njihovih lastnikov prisotne v organizaciji, verjeli, da so s tem zavarovani. Nekateri so bili mnenja, da je njihova raven varnosti precej visoka, ker ob nastopu zaposlitve podpišejo dogovore o varnem ravnanju s podatki, kar naj bi preprečevalo možnosti zlorab zaposlenih, a raziskava jasno pokaže, da to ne drži.

Z zadovoljstvom lahko povemo, da je bil odziv na poslani USB-ključček v bančnih in drugih finančnih ustanovah v skladu s pričakovano dobro razvito varnostno kulturo. V omenjenih organizacijah pomnilnega medija niso vstavljali v nobeno od naprav, priključenih na mrežo, prav tako naše sledenje ni zaznalo uporabe USB-ključka. V vseh primerih so pomnilni medij tudi uničili. Za določene panoge tako sklepamo, da je raven zavedanja in pripravljenosti na mogoče incidente višja. Nismo pa zaznali razlik v odstotku uporabljenega USB-ključka glede na velikost organizacije. Naleteli smo na primer, ko v organizaciji niso imeli vpeljane nobene varnostne politike, ravnali so le po zdravi pameti, kot je dejal sogovornik ob našem klicu.

V raziskavo smo zajeli dobro stoječa podjetja s solidnimi prihodki in posledično večjo izpostavljenostjo ter pričakovanji uporabnikov. Ob tem smo mnenja, da bi bili rezultati v primeru vključitve šibkejših podjetij lahko še slabši.

Vsekakor smo s pomočjo raziskave dobili dodatne dokaze, ki vodijo v potrditev izhodiščne trditve T2, saj izredno visok odstotek (> 90 %) uporabljenega USB-ključa jasno nakazuje slabo ozaveščenost zaposlenih v (osrednje)slovenskih organizacijah in obenem ponuja negativen odgovor na zastavljeno raziskovalno vprašanje R2.

Kot zanimivost naj omenimo še odziv ene od organizacij, ki ključka ni uporabila. S spremnim dopisom, da ključek ni njihov, so ga predali v obravnavo policiji. Nato smo zaznali večkratno uporabo ključka z IP-naslovnega območja, ki pripada Ministrstvu za notranje zadeve RS. Naslednji dan smo prejeli klic s policijske postaje, da so našli “naš” ključek, in želeli izvedeti naslov, na katerega naj nam ključek vrnejo.

3.3 Analiza učinka delavnic s pomočjo vprašalnikov

Zahvaljujoč inovativnemu poskusu družbenega inženiringa, v katerega je bila vključena tudi zdravstvena ustanova v Ljubljani, je ekipa Safe Mode od njih prejela povabilo, naj v praksi pokaže učinek delavnic ozaveščanja na zaposlenih.

V aprilu, maju in juniju 2016 smo izvedli serijo desetih delavnic ozaveščanja za 210 zaposlenih v tej organizaciji. Jeseni 2016 načrtujemo izvedbo delavnic še za vse ostale zaposlene s posebnim poudarkom na delavnicah za najvišje vodstvo.

Preden je organizacija poslala prvo vabilo za udeležbo na delavnicah, je približno 5000 zaposlenih, ki so uporabniki e-poštnega naslova organizacije, prejelo tudi vprašalnik, s pomočjo katerega smo želeli ugotoviti trenutno stanje glede ozaveščenosti in (na željo vodstva) tudi spoštovanja določenih pravil iz varnostnih politik.

Po zaključku delavnice smo vsem udeležencem zaključno anketo posredovali v pisni obliki (zaradi boljšega odziva). Namen zaključne ankete po delavnici je bil ugotoviti neposreden učinek vsebine delavnice na dejavnike, povezane z varovanjem informacij, ki smo jih navedli v prejšnjih poglavjih:

- mnenje o stanju varovanja informacij v organizaciji,
- odnos do skladnosti s politiko varovanja informacij,
- pripravljenost na morebitne varnostne incidente,
- zadovoljstvo z delavnico,
- želja po ponovni udeležbi na tovrstni delavnici.

Vodstvo organizacije je izpostavilo zahtevo po anonimnosti rezultatov vprašalnikov, ki smo jo med izvedbo raziskave dosledno spoštovali.

3.3.1 Teoretična podlaga sestave vprašalnikov

Vprašalnik pred delavnico ozaveščanja smo pripravili v spletni aplikaciji Google Forms. Ta omogoča preprost vnos in popravke vprašanj ter je dovolj zmogljiva, da pokrije naše potrebe za vprašalnik. Pri smernicah oblikovanja vprašanj smo želeli slediti načelom in priporočilom Dillmana in drugih [10], ki narekujejo predvsem oblikovno strukturo vprašalnika. Ugotovili smo, da je večina smernic zelo dobro zajetih v Google Forms, zato smo tudi drugi vprašalnik pripravili v Google Forms.

Žal smo po prvi delavnici ugotovili, da je težko pripraviti vse zaposlene do izpolnjevanja vprašalnika, ko enkrat zapustijo predavalnico (od 20 udeležencev jih je spletno anketo izpolnilo le 7). V nadaljevanju smo zato ob koncu vseh delavnic razdelili anketne liste na papirju z vprašanji iz priloge 2.

Vprašanja v obeh anketah so bila številčno omejena zaradi želje organizacije po čim manjši časovni obremenitvi zaposlenih. Tudi sami smo bili mnenja, da bi bila obsežnejša raziskava deležna manj odgovorov.

3.3.2 Vprašalnik pred delavnico ozaveščanja

Vprašalnik je pripravljen z namenom pridobiti splošen vpogled v trenutno stanje ozaveščenosti zaposlenih glede informacijske varnosti. Razposlan je bil na vse e-poštne naslove v organizaciji, prejeli pa smo 253 veljavnih odgovorov (od 256 skupaj prejetih), kar predstavlja soliden odziv oz. več kot 5 % zaposlenih v organizaciji.

Nabor vprašanj je vodja varovanja informacij organizacije predhodno skrajšal, vsebinsko dopolnil in dal končno potrditev.

Vprašalnik je sestavljen iz šestih vprašanj, ki so navedena v prilogi 1. Namen posameznih vprašanj je sledeč:

1. prvo vprašanje vzpostavi splošni kontekst poznavanja pravilnikov;
2. drugo vprašanje ima namen pridobivanja zaupanja zaposlenega s pozivom, naj pove, kaj ga pri delu muči oz. ovira;
3. tretje vprašanje neposredno poizveduje po do zdaj zaznanih incidentih;
4. četrto vprašanje posredno poizveduje, kako pogosto odnašajo delo domov (na delavnicah smo nato vprašali, ali to pomeni, da odnašajo domov oz. pošiljajo na zasebne elektronske naslove tudi podatke);
5. v petem vprašanju smo anketirance prosili za oceno števila gesel, ki jih uporabljajo. Vprašanje je bilo namerno odprtega tipa, da smo dobili dodatne kvalitativne ocene (npr. preveč gesel itd.);
6. zadnje, šesto vprašanje je bila poizvedba po deljenju gesel, ki je izpostavljeno kot ena ključnih težav v organizaciji. Vprašanje je namerno zaprtega tipa, da postavi navidezni okvir oz. nesprejemljiv odgovor (> 5), čeprav je v neskladju z varnostno politiko organizacije že kakršnokoli deljenje gesel (> 0).

Ključne ugotovitve analize vprašalnika pred izvedbo delavnic

- Zaposleni relativno slabo poznajo varnostne politike, sprejete v organizaciji.
- **12,3 %** zaposlenih različni pravilniki in varnostne politike ovirajo pri njihovem delu (nekompatibilnost sistemov, ščitenje osebnih podatkov, preveč gesel itd.).

- **21,7 %** jih je že bila priča varnostnemu incidentu (od zlorabe gesel za dostop med zaposlenimi in študenti do uhajanja občutljivih podatkov novinarjem itd.).
- Več kot polovica (**53 %**) zaposlenih delo odnaša domov (in včasih tudi občutljive podatke), vprašanje pa je, kako te podatke ščitijo doma.
- Večina zaposlenih uporablja premalo različnih gesel, torej so gesla enaka za več sistemov.
- **35,6 %** zaposlenih svoja gesla deli med seboj, kar pomeni, da je ravno toliko zaposlenih v prekršku glede na varnostno politiko uporabe gesel, kjer je zapisano, da se gesel ne sme deliti.
- Digitalnega certifikata, ki ga uporablja organizacija, ne priznava noben internetni brskalnik — zaposleni morajo pred vstopom dovoliti izjemo brskalniku, da nadaljuje naprej na poštni strežnik, s tem pa se zaposlene navaja na izjemno slabo navado, saj je nepotrjen certifikat eden najočitnejših znakov, da je lahko s spletno stranjo nekaj narobe oz. da gre za lažno stran.

3.3.3 Izvedba delavnic ozaveščanja

Delavnice so potekale v predavalnicah organizacije. Število udeležencev na posamezno delavnico smo za čim boljši učinek poskušali omejiti na približno 20, vendar žal na to nismo imeli neposrednega vpliva. Tudi osip je bil precejšen (udeleženci so se prijavljali, pa niso prišli), zato so odgovorni za izobraževanje postavili precej višjo omejitev prijav (50). Število udeležencev na posamezno delavnico je bilo tako med 7 in 40.

Ključne ugotovitve med izvajanjem delavnic

- Zaposleni so večkrat poudarili, da jim v določenih primerih ni omogočeno varno delo po vzoru najboljših praks.
- V primeru okužbe z izsiljevalskim virusom je IT-služba zaposlenim dala nov disk, reševanje podatkov pa je bilo prepuščeno njim samim (v tem primeru smo na pomoč priskočili predavatelji in rešili celotno bazo elektronske pošte, ki je vsebovala tudi večino izgubljenih datotek).
- Zaposleni so na delavnicah precej aktivno sodelovali, praktični prikazi so jim bili zanimivi, nekateri pa so navedli tudi nekaj svojih primerov iz domačega in službenega okolja.
- Prisotni so pokazali veliko zanimanja za delavnice na ožjih področjih, kjer bi posamezno problematiko lahko bolje razdelali (npr. na prihodnjih delavnicah).

- Zaposleni so večkrat postavili vprašanje o varnostnih kopijah za nekatere naprave in izpostavili problematiko dobave prenosnih medijev za izdelavo varnostnih kopij.
- Na splošno je prisotno mnenje, da bi nepoznan USB-ključek večina zaposlenih vstavila v računalnik in pregledala vsebino, čeprav so takšni ključki najbolj razširjena metoda okužbe z zlonamerno kodo.

3.3.4 Vprašalnik po delavnici ozaveščanja

Vprašalnik [priloga 2] je pripravljen z namenom analizirati učinek delavnice in predvsem vzpostaviti okvir, "kje bi želeli biti" v pogledu varovanja informacij v prihodnje. Vprašanja so bila pretežno zaprtega tipa. Kljub več vprašanj sta bila čas izpolnjevanja krajši (1—2 minuti) in vnos v spletni vmesnik hitrejši.

Namen posameznih vprašanj:

1. s prvim vprašanjem sprašujemo po lastnem mnenju anketirancev o stopnji poznavanja politike varovanja informacij;
2. drugo vprašanje predstavlja preusmeritev v prihodnje stanje in neposredno poizvedbo o učinku ozaveščanja;
3. v tretjem vprašanju želimo izvedeti osebno mnenje o pogosti kršitvi — odnašanju podatkov iz organizacije;
4. četrto vprašanje prepleta lastno mnenje z organizacijsko potrebo po prepošiljanju pošte, mogočih pa je več odgovorov, ki ustvarijo matriko mnenja v primerjavi s potrebo,
5. peto vprašanje se ponovno (kot pri vprašalniku pred delavnico) dotika kompleksnosti gesel, prepletanja vsebine delavnice, rezultatov prvega vprašalnika in pričakovanega ravnanja v prihodnje (mogočih več odgovorov);
6. šesto vprašanje je vrnitev na oceno splošne ravni varovanja informacij, temelječo na dosedanjih izkušnjah in vsebini delavnice;
7. sedmo vprašanje je namenjeno oceni delavnice, lestvica 1—6 je določena z namenom izognitve srednji vrednosti;
8. pri osmem vprašanju sprašujemo po lastnem mnenje o koristnosti tovrstne delavnice in pripravljenosti na ponovno udeležbo;
9. zadnje, deveto vprašanje je odprtega tipa in namenjeno komentiranju delavnice.

Pri vprašalniku pred delavnico smo do osebnih mnenj poskušali priti preko odprtih odgovorov, kjer so lahko anketiranci samostojno izrazili svoje mnenje. Pri večini vprašanj vprašalnika po delavnici pa smo poskušali pridobiti informacijo o njihovem prepričanju oz. lastnem

odnosu do varovanja informacij in skladnosti s politiko s pomočjo zaprtih vprašanj z mogočimi več odgovori (multiple choice).

Ključne ugotovitve po izvedbi delavnic

- **73,6 %** zaposlenih bi želelo bolje spoznati politiko varovanja informacij.
- **79,3 %** jih bo zdaj precej pozornejših na morebitne incidente, ki so bili predstavljeni na delavnici.
- **73,5 %** jih zdaj meni, da odnašanje poslovnih in osebnih podatkov pacientov iz organizacije ni dopustno, saj lahko pride do izgube podatkov.
- Skoraj polovica jih meni, da je pošiljanje elektronske pošte na zunanje strežnike nujno potrebno za opravljanje dela izven organizacije, saj jih službeni poštni predal preveč omejuje.
- Samo **8,1 %** jih še meni, da lahko svoja gesla delijo s sodelavci (pretežno, ker jim zaupajo).
- Delavnice so udeleženci zelo dobro ocenili (povprečna ocena **5,33** od 6).
- **93,9 %** zaposlenih bi se tovrstnih delavnic želelo udeležili tudi v prihodnje.

Navkljub določenim omejitvam raziskave s pomočjo vprašalnikov pred izvedbo delavnice ozaveščanja in po njej smo prišli do zanimivih rezultatov. Raziskavo bomo v jesenski seriji delavnic nadaljevali, jo po potrebi in zmožnostih razširili in tako morebiti prišli do novih dognanj.

Vsekakor lahko na tem mestu pritrdimo izhodiščni trditvi T3, saj je delavnica ozaveščanja (kot odgovor na raziskovalno vprašanje R3) pokazala, da ustrezno usposabljanje in ozaveščanje bistveno pripomoreta k varnejšemu delu zaposlenih, spodbudita zanimanje za tematiko, zmanjšata določene ranljivosti in preprečujeta udejanjanje določenih groženj.

4 Povzetek ugotovitev raziskav

Po uporabi treh različnih metod in analitičnih pristopov, ki izhajajo predvsem iz praktičnega oz. konkretnega poslovnega okolja, lahko ugotovimo, da zastavljena raziskovalna vprašanja prejmejo jasne odgovore in rezultati govorijo v prid potrditev izhodiščnih trditev. Poenostavljeno posploševanje seveda ni mogoče, kljub vsemu pa rezultati podajajo neko značilno predstavitev in sliko o stanju ozaveščenosti zaposlenih v določenem okolju.

Navedimo odgovore na posamezna raziskovalna vprašanja in povezane trditve, kot izhajajo iz rezultatov analiz:

R1: Kolikšen je delež človeškega dejavnika pri varovanju informacij?
T1: Človeški dejavnik je odgovoren za več kot polovico incidentov, povezanih z varovanjem informacij v organizaciji.

Rezultati na primeru organizacije govorijo v prid večinskemu deležu človeškega dejavnika. To pomeni, da je človek oz. zaposleni, ki delajo z informacijami, ključni odgovorni dejavnik tako za pozitivne kot negativne posledice (ne)ustrezne varnosti informacij in informacijskih sistemov.

R2: Ali so uporabniki v slovenskih organizacijah dovolj ozaveščeni glede varovanja informacij?
T2: Zaposleni v slovenskih organizacijah so premalo ozaveščeni glede varovanja informacij.

Raziskava je pokazala, da zaposleni v večini uspešnih slovenskih organizacij niso ustrezno izobraženi oz. dovolj ozaveščeni glede največjih potencialnih groženj in pravilnega ukrepanja ob srečanju z njimi. To velja tako za manjše kot velike organizacije, ne glede na dejavnost.

R3: Kako lahko učinkovito izboljšamo ozaveščenost zaposlenih v organizaciji?
T3: Za doseganje višje stopnje varovanja informacij v organizaciji je ozaveščanje zaposlenih ključnega pomena.

Kot izhaja iz rezultatov anket, predstavljajo delavnice ozaveščanja primeren in učinkovit način za dvig splošne ravni zavedanja varovanja informacij zaposlenih. Predvsem so nakazani porast pripravljenosti za skladno ravnanje, porast zanimanja za tematiko in večja pripravljenost za udeležbo na tovrstnih ozaveščanjih tudi v prihodnje.

Navedimo še nekaj dodatnih ugotovitev in mnenj, ki izhajajo iz vseh treh analiz, predstavljenih v nalogi:

- zgolj prisotnost standardov in varnostnih politik ne zagotavlja varnosti, **če zavest o pomenu varovanja informacij ni vključena v kulturo organizacije**;
- **zagotavljanje varnosti v organizaciji je stvar vseh zaposlenih in ne redkih posameznikov**;
- dokler se uporabniki ne bodo zavedali, kaj jim varnostne politike narekujejo, in tudi razumeli, kako te zahteve izpolnjevati, politike ne bodo imele učinka;
- uporabnikov ni smiselno siliti v prebiranje in učenje več deset stranskih politik, ampak jih je treba narediti bolj življenjske in jih uporabnikom predstaviti na njim razumljiv način;
- če z določenimi vpeljanimi ukrepi v organizaciji ne preprečujemo nastanka škodnih pojavov, ni smiselno, da ukrepe sploh vpeljujemo.

Učenje s pomočjo dinamičnih delavnic, s plastičnim in nazornim prikazom potencialnih groženj, vpeljava življenjskih varnostnih politik in preizkus razumevanja dokumentacije ter analitika napredka so ključni dejavniki pri zagotavljanju informacijske varnosti v organizacijah.

Da bi spremembe lahko začeli uvajati, je treba smiselno usmerjati in usposabljati miselnost vodstva, ki se pogosto osredotoča na drage tehnične rešitve, namesto da bi se lotilo strukturiranega dela z zaposlenimi. S pravilnim, preprostim in posledično jasnim izobraževanjem zaposlenih lahko ob bistveno nižjih stroških dosežemo enak učinek, kot bi ga lahko z vpeljavo tehnične rešitve.

5 Zaključek z diskusijo

Namen magistrskega dela je bil združiti večletno delo na različnih področjih široke teme varovanja informacij: upravljanja s tveganji, poznavanja standardov, tehničnih varnostnih rešitev in izvedbe delavnic ozaveščanja. Na podlagi osebnih izkušenj, aktivnega dela v številnih slovenskih podjetjih in organizacijah ter zbrane strokovne literature, raziskovalnih člankov in spletnih virov se je kot najprimernejša tema za nadaljnjo raziskavo izpostavil prav človeški dejavnik v sklopu varovanja informacij. Zahvaljujoč usmeritvam mentorja so omenjene teme prišle do skupne rdeče niti, katere temelj je prav ozaveščenost zaposlenih v slovenskih organizacijah.

Delo z zaposlenimi terja v prvi vrsti aktivno vključevanje vodstva tako v fazi opredeljevanja, kako upravljati varovanje informacij, v izvedbeni fazi, ko je treba identificirati informacijsko premoženje organizacije in ustrezno raven zaščite, v usklajevalni fazi, ko se ukrepi za ščitenje informacij v veliki meri prelijejo na papir v obliki varnostnih določil oz. politik, ter seveda pri namenjanju potrebnih človeških in finančnih virov za vse dejavnosti izboljševanja in dviga ravni informacijske varnosti v organizaciji.

Nadalje so potrebni dobro poznavanje tveganj, ki jim je organizacija izpostavljena, njihovo vrednotenje in ustrezno ukrepanje. Pristop k upravljanju tveganj mora biti sistematičen, celovit in ponavljajoč, skladno s hitrostjo razvoja tehnologije in pojavljanja novih tveganj v okolju, kjer organizacija deluje, pa naj bo to formalna struktura javne združbe ali dinamični svet visokotehnološkega start-upa.

Standardi, namenjeni varovanju informacij, s svojim skladnostno naravnanim pristopom pogosto ne dosegajo želenega učinka. Predstavljajo dobro prakso upravljanja varovanja informacij v procesno naravnanem svetu, ki temelji na načelih masovne proizvodnje, na vnaprej natančno določenih postopkih. Napredek tehnologije počasi raztaplja rigidnost ponavljajočih se procesov v obstoječih organizacijah. Potreben je nov, komplementaren pristop k varovanju informacij, ki bo bolj usklajen s spremembami v realnem času in nenehnimi inovacijami in spremembami v omreženem svetu, predvsem pa pristop, ki bo v ospredje postavil zaposlenega in njegovo zmožnost za sposobno, odgovorno in varno delo z informacijskim premoženjem organizacije.

Potrebno je, da vodstvo organizacije aktivno sporoča potrebe organizacije po varovanju informacij vsem zaposlenim, jih usmerja v zaščito in skrb za informacijsko premoženje, ki ga upravljajo, in jih nagrajuje za varno delo z informacijami ter inovativne rešitve in pristope, ki dvigujejo raven varnosti v organizaciji.

K sorodnim raziskavam želimo privabiti čim širši krog interesentov, zato je različica aplikacije za analizo tveganja [21] dostopna na naslovu http://sbr.bozic.si in brezplačno na voljo za raziskovalne namene morebitnim študentom, ki bi želeli preizkusiti metodologijo ali izvajati analize za študijske potrebe. Ker je aplikacija razvita z namenom prodaje na trgu, uporaba v komercialne namene ni dovoljena.

Kot informacijski strokovnjaki se moramo tudi sami osebno ozaveščati in pedagoško usposabljati za ustrezno posredovanje potrebnih znanj informacijske varnosti široki masi uporabnikov brez potrebnih predznanj o IT. Navsezadnje je od naše kakovosti prenosa znanja in poznavanja posledic informacijske varnosti in nevarnosti odvisna uspešnost ozaveščanja uporabnikov. V tem močno soodvisnem in interaktivnem odnosu med tehnologijo in človeškim faktorjem je prevladujoča odgovornost na naši strani.

V ilustracijo te odgovornosti je nazorna ugotovitev udeleženke delavnice v zdravstveni organizaciji:
"Živjo! Moram ti povedati, da je bilo včerajšnje predavanje med najboljšimi, kar sem jih kdaj poslušala v sklopu predavanj [organizacije], pa sem že skoraj 10 let pri hiši. Predavatelji so bili zelo dobri, predavanje je bilo zanimivo, tudi če nimaš pojma o informacijski varnosti ali nasploh o računalnikih, tako da same pohvale in še več takih predavanj!"

-- sporočilo udeleženke predavanja vodji službe izobraževanja

Naključna uporabniška navedba razbija mit, da je informacijska varnost nekaj, s čimer naj se ukvarjajo le informatiki. Če je vsebina plastično in zanimivo predstavljena, lahko doseže učinek in potrebno ozaveščanje o pomenu informacijske varnosti tudi pri uporabnikih brez obsežnejšega informacijskega znanja.

6 Literatura in viri

[1] ISO/IEC 27001:2013 Information security management system: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[2] K. Zupan, F. Božič, Ž. Primc: Dovzetnost slovenskih podjetij za napade s pomočjo družbenega inženiringa — Zbornik UM-FVV, 2015.

[3] ISO 22301:2012 — Societal security — Business continuity management systems: http://www.iso.org/iso/catalogue_detail?csnumber=50038

[4] S. Kraemer, P. Carayon: Human error and violations in computer and information security, Applied Ergonomics, 2007.

[5] SI-CERT Poročilo o omrežni varnosti za leto 2015: https://www.cert.si/letna-porocila-o-omrezni-varnosti/

[6] R. Anderson et al.: Measuring the Cost of Cybercrime; The Economics of Information Security and Privacy, 2013.

[7] F. Božič: Risk Assessment Accelerator; aplikacija za analizo tveganja, 2010—2015.

[8] B. Bulgurcu, H. Cavusoglu, I. Benbasat: Information Security Policy compliance: An empirical study of rationality-based beliefs and information security awareness.

[9] IBM, Ponemon: 2015 Cost of Data Breach Study: Global Analysis.

[10] Dillman D. et al.: Principles for Constructing Web Surveys, 1999.

[11] Price-Waterhouse-Coopers: The Global State of Information Security® Survey 2016.

[12] COBIT 5 for Information Security: http://www.isaca.org/cobit/pages/info-sec.aspx

[13] COBIT 5: Človeški dejavnik v upravljanju varovanja informacij organizacije: http://www.isaca.org/Journal/archives/2013/Volume-6/Pages/Revisiting-the-Human-Factor-in-Organizational-Information-Security-Management.aspx

[14] SANS Top 20 Critical Security Controls.

[15] PCI-DSS: https://www.pcisecuritystandards.org/pci_security/

[16] ISF Standard of Good Practice for Information Security: https://www.securityforum.org/tool/the-standard-of-good-practice-for-information-security/

[17] Stanton et al.: Analysis of End User Security Behaviors; Computers and Security (24:2), pp. 124—133, 2005.

[18] N. Gibbs: COBIT 5 for Risk, IIA International Conference, Vancouver, Canada, July 2015.

[19] Organization for economic co-operation and development [OECD]. Guidelines for the security of information systems and networks, 2002.

[20] B. Lobnikar, K. Prislan, B. Markelj, E. Banutai: Informacijsko-varnostna ozaveščenost v javnem in zasebnem sektorju v Sloveniji; Varstvoslovje, 14(3), 345—363.

[21] F. Božič, M. Potočnik: Aplikacija za analizo tveganja Silver Bullet Risk: http://sbr.bozic.si

[22] M. E. Whitman: Enemy at the Gate: Threats to Information Security; Communications of the ACM, 2003.

[23] J. J. Gonzalez, A. Sawicka: A Framework for Human Factors in Information Security; WSEAS Conference on Inf. Security, Rio De Janeiro, 2002.

7 Priloge (tabele, vprašalniki)

7.1 Priloga 1 — Anketa pred delavnico

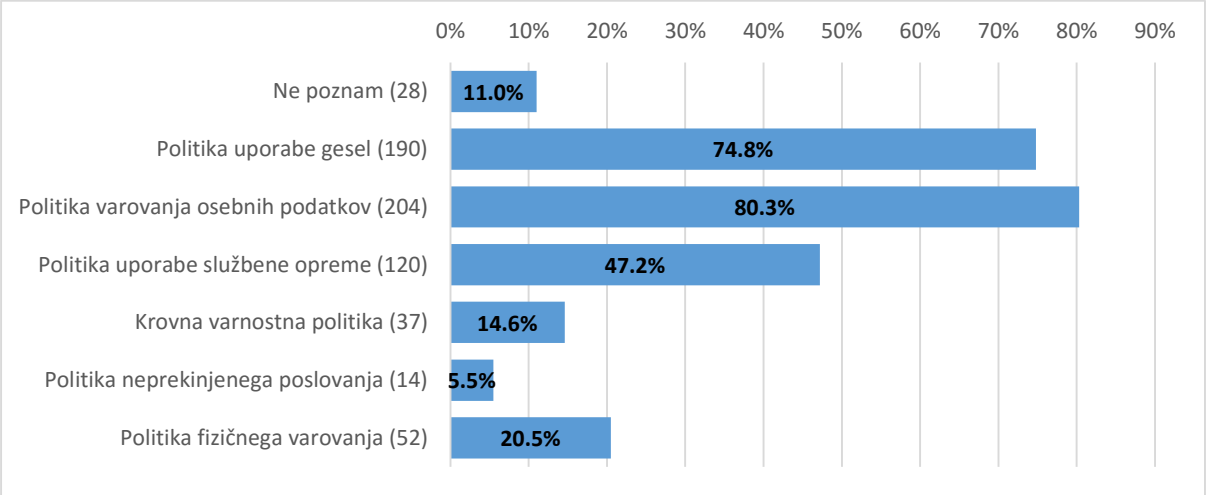
1	Katere varnostne politike in pravilnike v vaši organizaciji poznate? ▫ Ne poznam ▫ Politika uporabe gesel ▫ Politika varovanja osebnih podatkov ▫ Politika uporabe službene opreme ▫ Krovna varnostna politika ▫ Politika neprekinjenega poslovanja ▫ Politika fizičnega varovanja ▫ Drugo
2	Ali vas pri vaših poslovnih procesih ovira kateri od pravilnikov ali varnostnih politik sprejetih v organizaciji? Če da, kateri to so in v katerem delu vas ovirajo? ● Ne ● Da [ ]
3	Ste že bili priča varnostnemu incidentu? ● Ne ● Da [ ]
4	Kako pogosto odnesete delo domov? ● Dnevno ● Tedensko ● Mesečno ● Nikoli
5	Približno koliko različnih gesel uporabljate v poslovnem in zasebnem okolju? [ ]
6	Koliko sodelavcev pozna katero izmed vaših gesel? ● Nihče ● 1—2 ● 3—5 ● Več kot 5

7.2 Priloga 2 — Anketa po delavnici

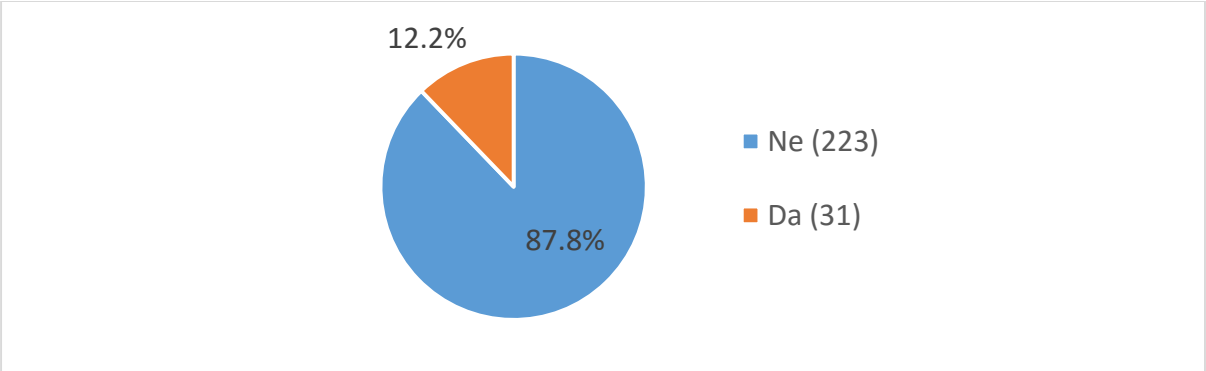
1	Kako dobro poznate politiko varovanja informacij? ● Dobro poznam ● Bi želel bolj podrobno spoznati ● Ne poznam
2	Boste v prihodnje bolj pozorni na morebitne varnostne incidente? ● Ne, ker ni potrebno ● Ne, ker sem že sedaj dovolj ● V manjši meri ● Da, zelo ● Drugo:
3	Se vam zdi primerno odnašati poslovne podatke ali osebne podatke pacientov izven organizacije? ● Da, saj moram delo narediti tudi izven delovnika ● Da, ker ščitim zaupnost podatkov ● Ne, saj lahko pride do izgube podatkov ● Ne, a količina dela to zahteva ● Drugo:
4	Prepošiljanje elektronske pošte na zunanje naslove (možnih več odgovorov): ▢ Je potrebno zaradi prevelikih omejitev poštnega sistema ▢ Je včasih nujno potrebno ▢ Nikakor ne sme vsebovati osebnih podatkov ▢ Se mi ne zdi pametno zaradi morebitne kršitve zaupnosti podatkov ▢ Se mi ne zdi sporno ▢ Ni dovoljeno ▢ Drugo:
5	Gesla za dostop do aplikacij in sistemov (možnih več odgovorov): ▢ So lahko enaka za več aplikacij ▢ Lahko zaupam sodelavcu/sodelavki ▢ Morajo biti različna ▢ Morajo biti dovolj kompleksna ▢ Je potrebno varovati pred sodelavci ▢ Drugo:
6	Ali menite, da je v vaši organizaciji ustrezno poskrbljeno za varovanje informacij? ● Preveč ● Da, odlično ● Dobro ● Srednje dobro ● Slabo ● Sploh ni poskrbljeno
7	Kako bi ocenili današnjo delavnico? 1 .. 2 .. 3 .. 4 .. 5 .. 6
8	Bi se želeli udeležiti tovrstnih delavnic tudi v prihodnje? ● Ne, ker niso koristne ● Ne, nimam časa ● Ne vem ● Da
9	S čim ste bili na izpopolnjevanju zadovoljni oz. kaj ste pogrešali?

7.3 Priloga 3 – Rezultati ankete pred delavnico(n = 253)

1. Kako dobro poznate politiko varovanja informacij?



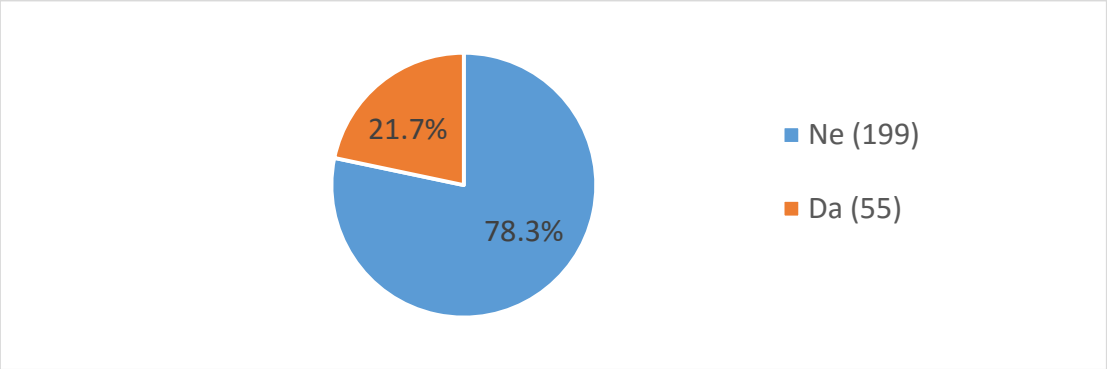
2. Ali vas pri vaših poslovnih procesih ovira kateri od pravilnikov ali varnostnih politik, sprejetih v organizaciji? Če da, kateri to so in v katerem delu vas ovirajo?



Opisni odgovori:

- Omejenost uporabe elektronske pošte z domeno [org].si.
- Preštevilna gesla.
- Zelo omejena možnost dela od doma, zelo omejeno uporaben spletni poštni vmesnik.
- Preprečitev dostopa do Facebooka (in nekaterih drugih družbenih omrežij) onemogoča dostop do nekaterih vsebin, ki so za našo dejavnost (promocija zdravja pri delu) zanimive, a so dostopne samo preko tega medija, hkrati pa to ovira tudi uporabo teh novih medijev za naše potrebe (različne kampanje za ciljne skupine zaposlenih, ki so dosegljive pretežno preko teh medijev (npr. samozaposleni v kulturi, medijih, prekarni mladi delavci itd.)).
- Zaradi številnih gesel in počasnega odpiranja programov se naročanje krvnih preiskav zavleče do onemoglosti, pacient lahko že izkrvavi, mi pa se vedno nismo poslali krvnih vzorcev, ker pacient se ni vnesen v sistem ali pa se birpis ravno updata, mi pa nujno nekaj potrebujemo.
- Nimam vpogleda v mikrobiološke izvide bolnikov, ki so na naš oddelek sprejeti z drugega oddelka (za potrebe preprečevanja boln. okužb), zato informacije pridobivam preko službenega telefona ali fotokopij ali faksa.
- Pravilniki o uporabi opioidnih zdravil in zdravil z visokim tveganjem.
- Varovanje podatkov.
- Ne moremo dostopati do podatkov o pacientovem zdravljenju, ker nimamo vpogledov , tako kot je bilo to mogoče v BISU.
- Ne vem, kakšno ime ima ta politika, a npr. nedostopnost bolnikovih izvidov iz drugih enot.
- Dostopnost do službenega računalnika od doma; online pomoč za analizatorje proizvajalca.
- Varovanje osebnih podatkov.
- Prepogosto je treba menjati gesla. 2. Gesel je (pre)več (za vsako aplikacijo svoje, namesto enega splošnega), npr. bolnišnični informacijski sistem, laboratorijski informacijski sistem, EDS, Webpis ...
- Varovanje osebnih podatkov.
- Gesla, ne morem si zapomniti 20 zapletenih gesel.
- Preveč različnih gesel.
- Zdravstveni delavec bi moral imeti dostop do vseh podatkov o nekem pacientu. npr. veš, kakšne so njegove pljučne funkcije, ne moreš pa pridobiti podatka o vrednosti njegovega Hb. Na Golniku temu ni tako!
- Ščitenju zasebnosti pacientov, učinkovitem komuniciranju ...
- Vsakokratno spreminjanje varnostnih gesel in uporaba posebnih gesel za oddelek, kjer trenutno krožimo – v primeru dežurstva pa nimam dostopa do podatkov v rednem računalniškem programu na drugih oddelkih, kjer tudi dežuram
- Gesel. Uporabniki ves čas menjamo računalnike. Potreba po hitrem odzivu.
- Varovanje gesel, varovanje osebnih podatkov, fizično varovanje.

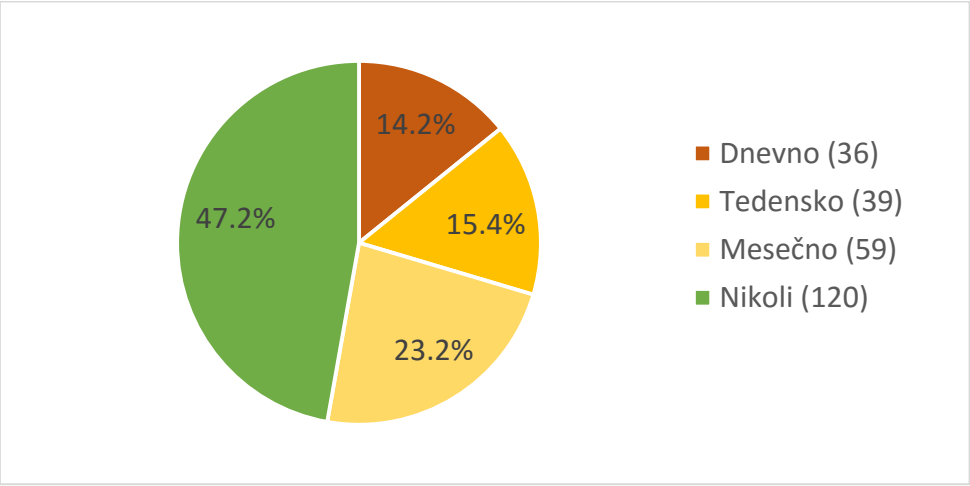
3. Ste že bili priča varnostnemu incidentu? Kakšnemu?



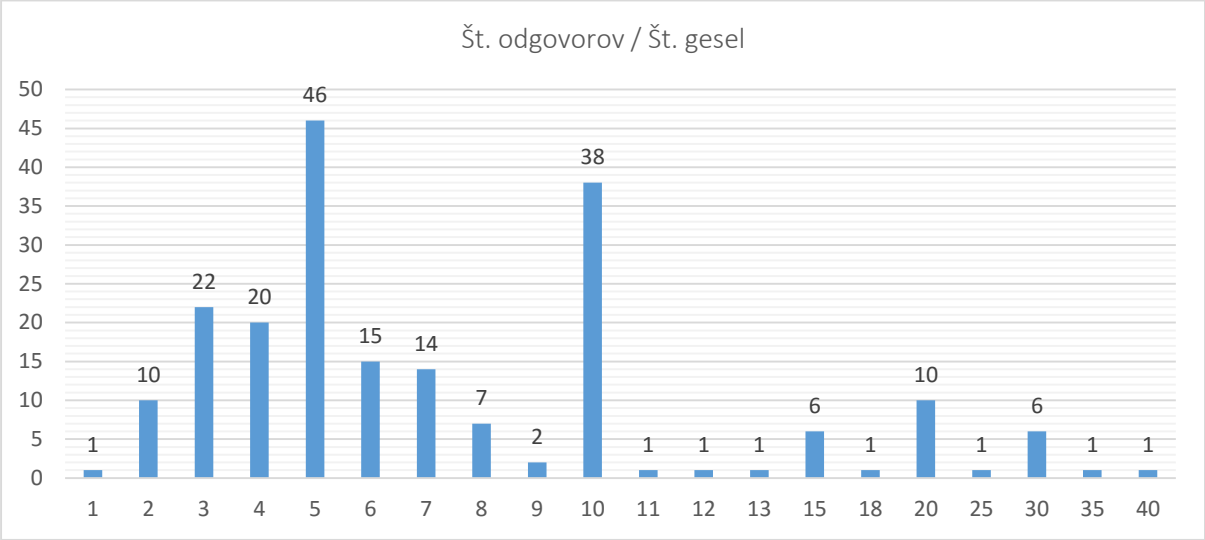
Opisni odgovori:

- Izguba podatkov.
- Zloraba zdravniškega gesla.
- Fizični napad pacienta.
- Brskanje izven kompetenc.
- Na nekaterih oddelkih nimajo spletne aplikacije MBX za vpogled v mikrobiološke izvide, zato jim na oddelke pošiljamo fotokopije izvidov bolnikov. Pred leti sem v garderobnem prostoru opazila, da je nekdo pustil cel kup različnih izvidov, na klopi.
- Nekateri zdravniki ne uporabljajo profesionalnih kartic, ampak za to zadolžijo druge.
- Delo v IS z "enotnim geslom" enote, posojanje osebnih gesel za vstop v IS sodelavcem, dodeljevanje pooblastil za vstop v IS "po dogovoru" (problem: neusklajeni uporabniški profili v UKCL).
- Deljenje gesel, nezaklepanje računalnika ob zapustitvi delovnega mesta ipd.
- Zloraba receptov oz. zdr. žiga.
- Kraja osebnih stvari v garderobnih omaricah sodelavcev.
- Nepokreten bolnik se, ležeč na postelji/vozičku, ni želel odmakniti izpred naše službe. Je protestiral. Vključili smo varnostno službo, varuha človekovih pravic, policijo ...
- Pacient ni želel, da se ga pokliče po imenu in priimku.
- Na infekcijski kliniki so študenti prišli do kritičnih informacij o svojem sošolcu.
- Vsakodnevno dajanje informacij o bolnikovem stanju svojcem po telefonu.
- Intervencija varnostnika.
- Uhajanje osebnih podatkov novinarjem.
- Napad spremljevalca na zdr. osebje.
- Padec pacienta, nepravilna aplikacija zdravila.
- Kraja denarnice ...
- Izjava pacientov o omejitvi obiskov, osebi, ki ni bila na seznamu, nisem povedala, kje leži oseba, tudi osebno se je oglasila, zahtevala je mojo vodjo, ki je še bila takrat v službi, menim, da še vedno informacije najlažje dobijo prek telefona, kar seveda ni dobro, saj je težko zaščititi tako paciente kot zaposlene.
- Fizični napad pacienta na zaposlene.
- Zaposleni si med seboj izposojajo gesla za službene programe.
- Zloraba uporabniškega imena pri pregledovanju RTG-slik pacienta.
- Pacient domov odšel z IV-kanalom.
- Neavtoriziran vstop v informacijski sistem, fizično nasilje nad zaposlenim.
- Zloraba osebnih podatkov.

4. Kako pogosto odnesete delo domov?



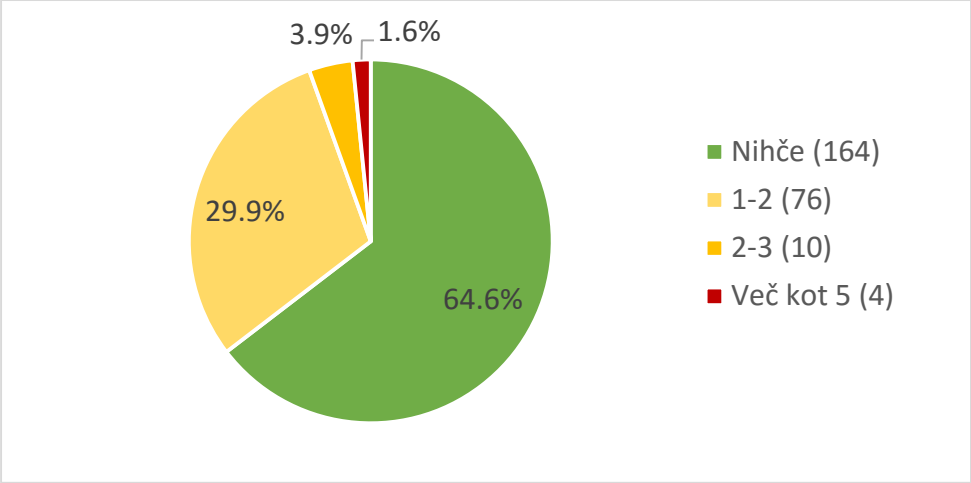
5. Približno koliko različnih gesel uporabljate v poslovnem in zasebnem okolju?



Nekaj opisnih odgovorov:

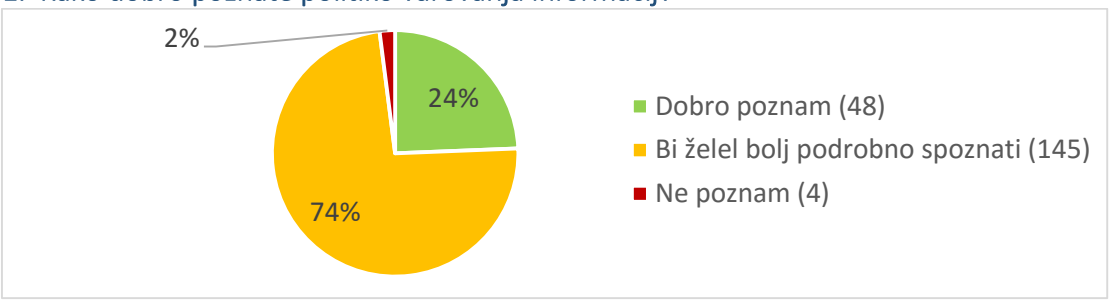
– Preveč (8–10)
– Malo morje – nad 30!
– Ufff, preveč (6) v poslovnem.
– Preveč.
– Niti ne vem točno, definitivno preveč.
– V zasebnem veliko več kot poslovnem.

6. Koliko sodelavcev pozna katero izmed vaših gesel?

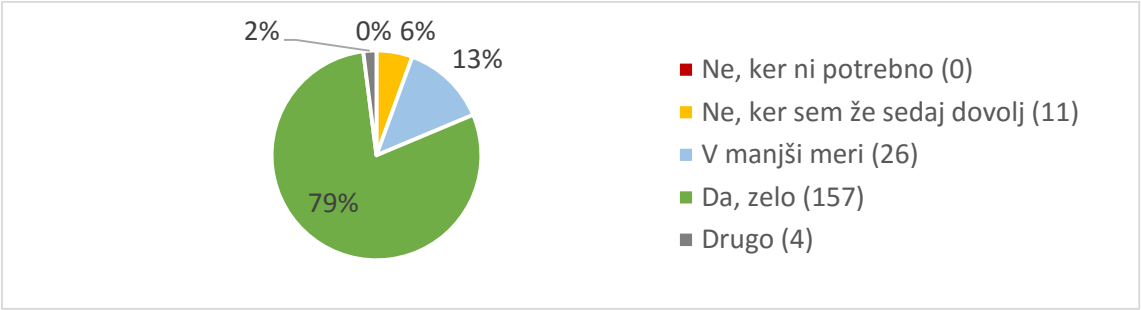


7.4 Priloga 4 – Rezultati ankete po delavnici (n = 198)

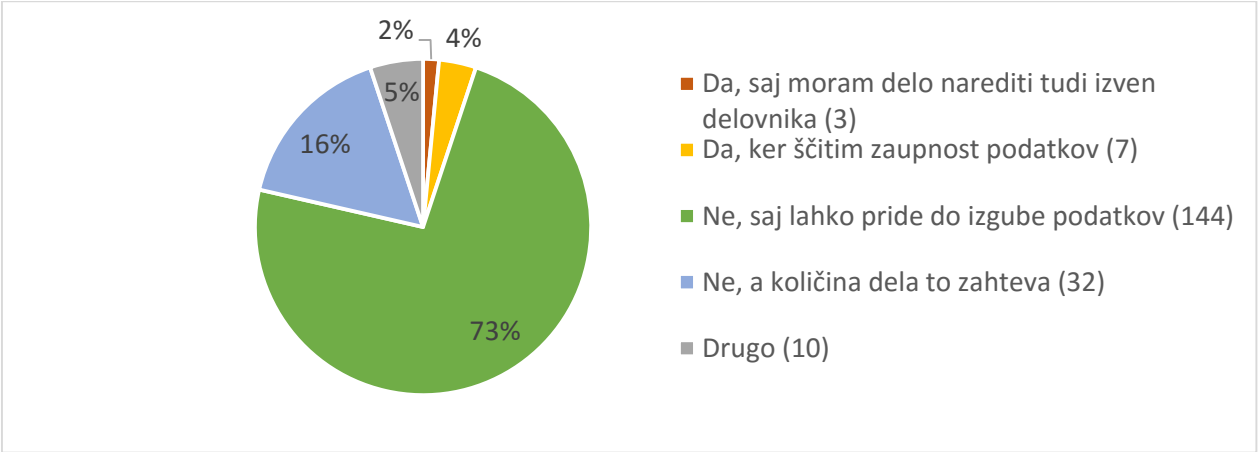
1. Kako dobro poznate politiko varovanja informacij?



2. Boste v prihodnje bolj pozorni na morebitne varnostne incidente?

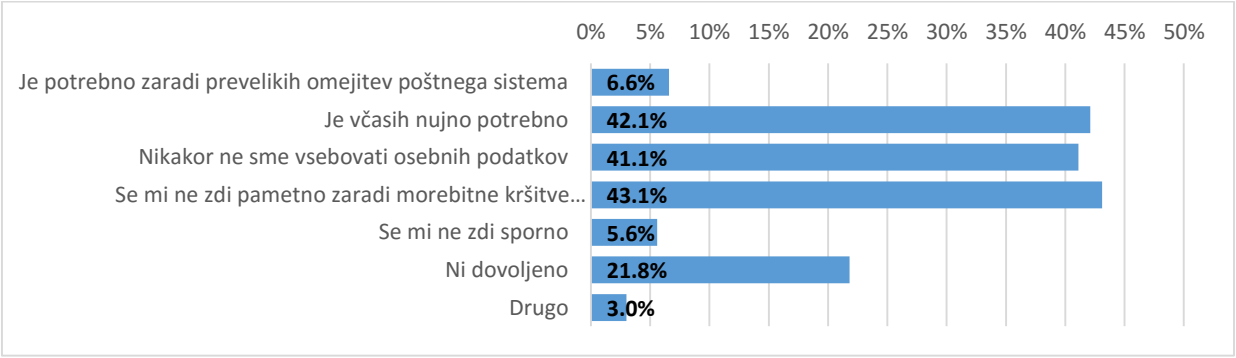


3. Se vam zdi primerno odnašati poslovne podatke ali osebne podatke pacientov izven organizacije?



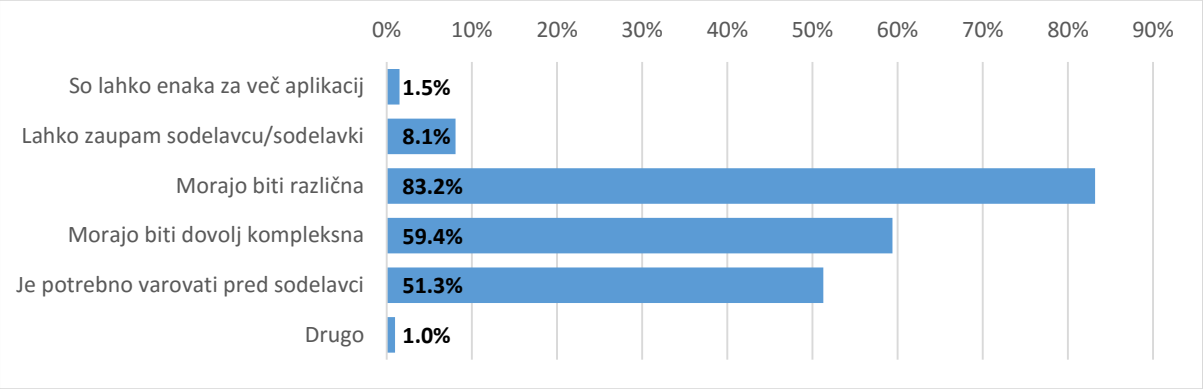
4. Prepošiljanje elektronske pošte na zunanje naslove:

(mogočih več odgovorov)

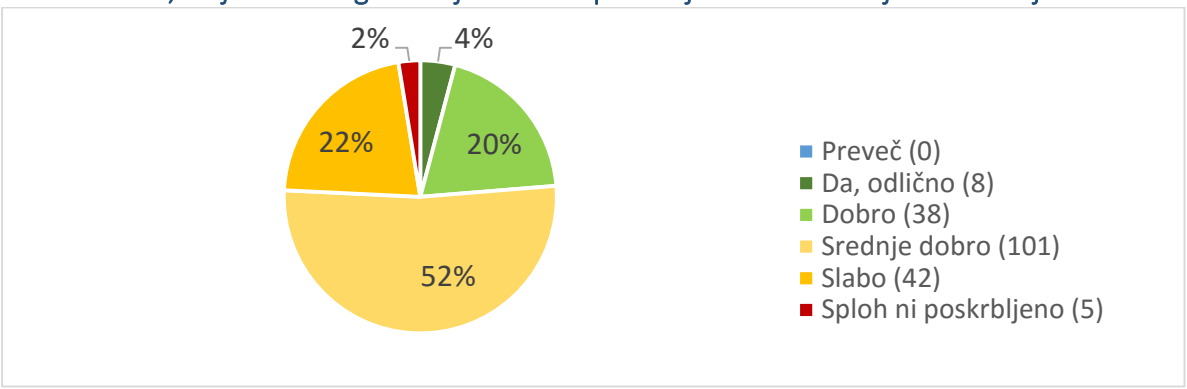


5. Gesla za dostop do aplikacij in sistemov:

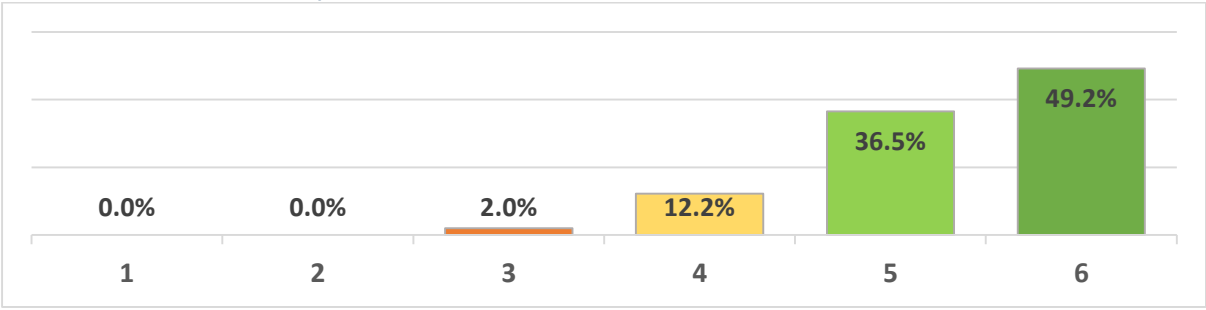
(mogočih več odgovorov)



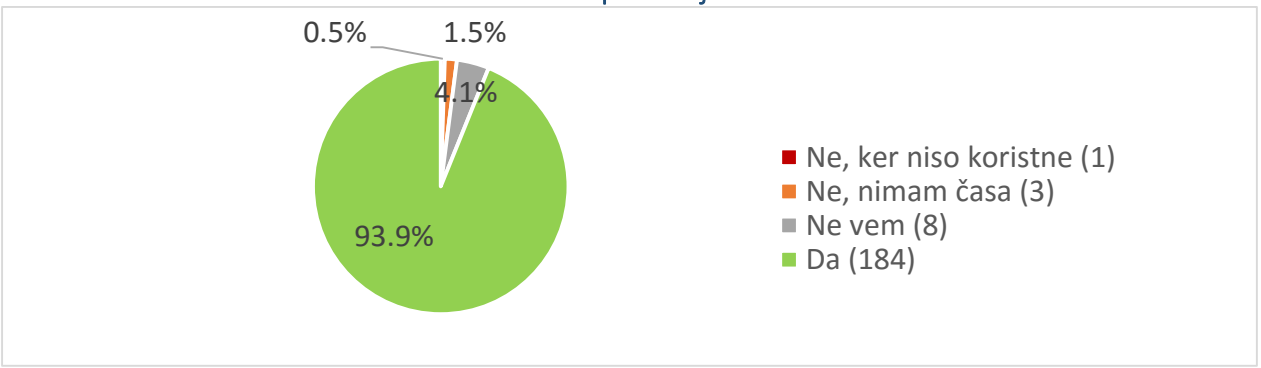
6. Ali menite, da je v vaši organizaciji ustrezno poskrbljeno za varovanje informacij?



7. Kako bi ocenili današnjo delavnico?



8. Bi se želeli udeležiti tovrstnih delavnic tudi v prihodnje?



9. S čim ste bili na izpopolnjevanju zadovoljni oz. kaj ste pogrešali?

- Z vsem.
- Osnovne informacije bi morale preiti do vseh sodelavcev.
- Uvod je bil dober, pri naštevanju posameznih varnostnih kršitev oz. vdorov pa bi bilo predavanje dobro "zabeliti" s konkretnimi incidenti!
- Na prihodnji delavnici mogoče več poudarka na praksi
- Več prikazov primerov, praktična navodila za vsakdanjo uporabo (gesla, pdf datoteke ...).
- Več časa za praktične prikaze.
- Print prezentacije.
- Vse ok!
- Večkrat izobraževati o novih oz. novostih zlorab.
- O sistemih v [org] – varnost – informacijske hiše.
- Vse super, še tako naprej!
- Konkretni primeri, kaj lahko naredimo konkretno.
- Vse je bilo v redu.
- Ponazoritev s primeri.
- Vse super, predstavljeno zelo izčrpno.
- Več primerov iz naše organizacije (primerov iz našega delovnega okolja).
- Interakcijo v smislu skupinske debate ali brainstorminga.
- Všeč mi je bilo, da je prikaz tudi praktičen (filmček, prisluškovalna napravica ...) in ne le teorija! Hvala!
- Dobra predstavitev.
- Zelo zanimiva delavnica.
- Zelo dobri praktični primeri in razlage.
- Vse ok.
- Razlaga s primeri iz življenja.
- Predstavitev tematike.
- Zadovoljen z izvedbo, zajeto dovolj veliko področje.
- Dobro izpostavljene izrabe osebne poti, zanimivi filmi za nazoren prikaz.
- Je dober začetek.
- Nazorno prikazano.
- Predstavitev primerov iz prakse.
- Delavnica mi je bila všeč ...
- Zelo pohvalno je moja ocena.
- Pohvalno.
- Zadovoljen s celotnim predavanjem.
- Praktični prikazi – primeri ...nasveti.
- Izpopolnjevanje na splošno, morda več primerov z imeni virusov ... iz konkretnega okolja [org].
- Zadovoljna – veliko novih informacij.
- Premalo uporabno za konkretno delovno področje (zdravstvo).
- Več časa za tolikšno količino informacij in pisno obliko.
- Všeč so mi bila nazorna, z videi obdana tematika in primeri, taki praktični. Super!
- Praktično izvajanje (prikaz ukrepov v primeru "zlorabe" – okužbe s kriptovirusi); več časa, a tolikšno količino informacij; en kratek odmor med 1,5 h delavnico!
- Predvsem s kratkim filmom. Lahko bi bil še kakšen več zaradi boljše predstave. Hvala.
- Z vsem, nič nisem pogrešala; zanimivo.
- Več vsebine za zaščito pri brskanju po internetu, možnosti shranjevanja, brisanje, zasebnosti.
- Izvedeli nekaj novega, kar nismo poznali, vsekakor bomo pozornejši.
- Da ni bilo samo teoretično, ampak tudi praktično prikazano, kako je s problematiko.
- Zabavna predstavitev in razumljivo podajanje tematike.
- Nič novega, vse dostopno tudi drugje.
- Več uporabnih informacij izključno iz [org], drugače pa dobro predavate.
- /
- Da ste nas poučili o novih tehnologijah.
- Razlaga na primeru!
- Vse ok.
- Še kar v redu predstavljeno. Vendar bi morali več poudarka nameniti zaščiti v zdravstvu! Predvsem bi bilo koristno posredovati čim več primerov, ki se dogajajo, in rešitve zanje, ki se jih verjetno večinoma ne zavedamo.
- S predstavitvijo in filmčki.
- Več praktičnih primerov, manj teorije.
- Dobra predstavitev.
- Morda ne morem popolnoma slediti.
- Še več praktičnih primerov.
- Učinkovito ravnanje z gesli, zlonamerna oprema.
- Praktične razlage in primeri.
- Podane informacije so zanimive.
- Pridobili smo vse potrebne in zanimive informacije.
- Bila je retorično odlična, podajanje zanimivih zadev.
- Pogrešali kakšen material, osnovne informacije s predavanja.
- Z informacijami o mogočih zlorabah.
- Ok.
- Primeri, kako lahko pride do incidenta.
- Da sem informirana splošno, podrobneje bi se informirala na to temo.
- Razumljivo in dobro predstavljeno.
- Praktični prikazi.
- Konkretni primeri iz prakse.
- Razumljivost in predstavitve (film).
- Bilo je zanimivo.
- Več besed o naših internih sistemih, kako delujejo. Saj se mi zdi, da premalo vemo, kako delujejo in jih tako težje razumemo.
- Več primerov, kaj in kako se virus namesti –> primeri priponk, lažnih spletnih strani ...
- Vse je bilo super.
- Več praktičnih primerov in nasvetov.
- Več konkretnih navodil.
- Razlago.
- Všeč so mi praktični primeri.
- Še natančneje ali več časa za podajanje vsebine.
- Še več o zdravstvu.
- Zadovoljna z vsem.
- S seznanitvijo različnih nevarnosti v svetu tehnologije.
- Dobrodošel bi bil še kakšen video. Predavalnica je neustrezna.
- O pasteh zlorab bi pa se moral [org] bolj posvečati varovanju e-pošte – vsaj to.
- Predstavitev vsebine zelo dobra.
- Še več realnih primerov.
- S praktičnim prikazom zadovoljna!
- Vse je bilo v redu in zanimivo.
- Konkretne rešitve.

7.5 Priloga 5 – Nabor groženj

1.01	Naravna nesreča (potres, vihar, poplava, udar strele)
1.02	Vpliv okolja (požar, izliv vode, temperatura, vlaga, umazanija, magnetno polje)
1.03	Zlonamerni napadi (vandalizem, vojna/nemiri, kraja)
1.04	Nepooblaščen dostop do okolja in infrastrukture
1.05	Izpad oskrbe z energijo in drugimi viri (elektrika, voda, plin)
2.01	Pomanjkanje osebja
2.02	Nenamerne napake pri delu
2.03	Neizvajanje varnostnih določil
2.04	Namerno kršenje varnostnih določil
2.05	Zlorabe
2.06	Osebje ne poroča o odkritih incidentih in varnostnih pomanjkljivostih
2.07	Neustrezna strokovna znanja osebja
2.08	Pomembna delovna mesta zasedajo neprimerni ljudje
3.01	Naravne nesreče (potres, poplava, vihar, udar strele)
3.02	Negativni vplivi okolja (požar, temperatura, voda, vlaga, prah, magnetno polje)
3.03	Zlonamerne poškodbe (kraja, vandalizem, stavke, nemiri)
3.04	Nedelovanje strojne opreme
3.05	Nezadovoljivo delovanje strojne opreme (počasno ali nepričakovano)
4.01	Izguba podatkov
4.02	Obnovitev delovanja po nesreči ne uspe
4.03	Odpoved programske opreme
4.04	Napačni rezultati obdelave ali zajema podatkov
4.05	Lažno predstavljanje ob prijavi v sistem
4.06	Nepooblaščena uporaba programov ali vpogled in spreminjanje podatkov
4.07	Nepooblaščene spremembe programov in nastavitev
4.08	Zloraba pooblastil
4.09	Kraja podatkov
4.10	Zanikanje udeležbe v transakciji
4.11	Uporaba nedovoljene programske opreme
4.12	Delovanje zlonamerne programske opreme
4.13	Kraja programske opreme (poslovna skrivnost, konkurenčna prednost)
5.01	Negativni vplivi okolja (požar, temperatura, magnetno polje ...)
5.02	Zlonamerne poškodbe (kraja, vandalizem)
5.03	Nedelovanje komunikacij
5.04	Nezadovoljivo delovanje komunikacij (počasno, napake pri prenosu)
5.05	Nepooblaščen dostop do komunikacij
5.06	Izguba zaupnosti (kraja podatkov, prestrezanje, družbeni inženiring, sleparjenje protokolov)
6.01	Naravna nesreča (potres, poplava ...)
6.02	Vplivi okolja (požar, izliv vode, temperatura, vlaga, umazanija, magnetno polje)
6.03	Kraja podatkov/dokumentov
6.04	Nepooblaščen dostop do podatkov, dokumentov, sporočil
6.05	Nepooblaščeno spreminjanje podatkov
6.06	Izguba razpoložljivosti za pooblaščene uporabnike
6.07	Izguba podatkov zaradi nepazljivosti
6.08	Nerazpoložljivost varnostnih kopij
6.09	Nepooblaščeno pregledovanje, presnemavanje, odstranjevanje arhiviranih dokumentov
6.10	Okvare v varnostnih kopijah
6.11	Dostop vzdrževalcev/čistilcev do podatkov/dokumentov
6.12	Propadanje dokumentov na papirju
6.13	Propadanje medijev za shranjevanje podatkov
6.14	Uporaba neveljavnih dokumentov
7.01	Kršitve pogodbenih in tretjih oseb
7.02	Kršitve zakonodaje